# Cisco Cloud APIC コンポーネントの設定



## Cisco クラウド APIC の設定について

Cisco Cloud APIC GUI または REST API を使用して Cisco Cloud APIC コンポーネントを作成します。ここでは、設定、アプリケーション管理、運用、および管理コンポーネントの作成方法について説明します。

（注）

- ロードバランサとサービス グラフの設定については、レイヤ 4 から レイヤ 7 サービスの展開 を参照してください。
- ナビゲーションや構成可能なコンポーネントのリストなどの GUI については、Cisco Cloud APIC GUI の概要 を参照してください。

## GUI を使用した Cisco Cloud Cisco APIC の設定

### Cisco Cloud APIC GUI、リリース 4.2(2) 以前を使用したテナントの作成

このセクションでは、Cisco Cloud APIC GUI を使用したテナントの作成方法について説明します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

**[アプリケーション管理（Application Management）]** オプションのリストが **[インテント（Intent）]** メニューに表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[テナントの作成（Create Tenant）]** をクリックします。**[テナントの作成（Create Tenant）]** ダイアログ ボックスが表示されます。

**ステップ 4** 次の *[*テナントの作成（*Create Tenant*）*]* ダイアログボックスのフィールドの表に示されているように、各フィールドに適切な値を入力し、続行します。

**表 *1:* テナント ダイアログボックス フィールドの作成**

| **[プロパティ（Properties）]** | 説明 |
|---|---|
| **名前（Name）** | テナント名を入力します。 |
| **説明** | テナントの説明を入力します。 |
| **設定** | |
| **セキュリティ ドメインの追加** | セキュリティ ドメインを追加するには、次の手順を実行します。<br>**1.** **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。<br>**2.** セキュリティ ドメインをクリックして選択します。<br>**3.** **[選択（Select）]** をクリックして、セキュリティ ドメインをテナントに追加します。 |
| **信頼できるテナント** | **[有効]** チェックボックスをクリックしてオン(デフォルト) またはオフにします。オンにすると、**信頼できるテナント**が有効になります。 |
| **クラウドアカウントID** | クラウド アカウント ID を入力します。 |

**ステップ 5** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI、リリース 4.2(3) 以降を使用したテナントの作成

このセクションでは、Cisco Cloud APIC GUI を使用したテナントの作成方法について説明します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

**[アプリケーション管理（Application Management）]** オプションのリストが**[インテント（Intent）]** メニューに表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[テナントの作成（Create Tenant）]** をクリックします。**[テナントの作成（Create Tenant）]** ダイアログ ボックスが表示されます。

**ステップ 4** 次の *[テナントの作成（Create Tenant）]* ダイアログボックスのフィールドの表に示されているように、各フィールドに適切な値を入力し、続行します。

**表 *2*:テナント ダイアログボックス フィールドの作成**

| **[プロパティ（Properties）]** | **説明** |
|---|---|
| **名前（Name）** | テナント名を入力します。 |
| **説明** | テナントの説明を入力します。 |
| **設定** | |
| **セキュリティドメインの追加** | セキュリティ ドメインを追加するには、次の手順を実行します。<br>1. **[セキュリティ ドメインの追加（Add Security Domain）]**をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。<br>2. セキュリティ ドメインをクリックして選択します。<br>3. **[選択（Select）]**をクリックして、セキュリティ ドメインをテナントに追加します。 |
| **AWSアカウントID** | クラウドアカウント ID を入力します。 |
| **アクセスタイプ** | クリックしてテナント タイプを有効にします。<br>• 信頼できない<br>• 信頼できる<br>• 組織 |

**ステップ 5** 設定が終わったら [Save] をクリックします。

# リリース 4.2(2) 以前のテナント AWS プロバイダーを設定する

### 始める前に

- AWS プロバイダーは、インフラ テナント用に自動設定されます。インフラ テナント用に AWS プロバイダーを構成するために何もする必要はありません。
- すべての非インフラ テナントの場合、AWS プロバイダーは信頼できるテナントまたは信頼できないテナントとして設定されます。資格情報の管理は簡単ではないため、信頼できるテナントを使用することをお勧めします。また、各テナントは個別の AWS アカウントに属している必要があります。複数のテナントで同じ AWS アカウントを共有することは許可されていません。

  信頼できるテナントの場合、最初に Cisco Cloud APIC が展開されているアカウント (インフラ テナントのアカウント) との信頼関係を確立します。信頼関係を確立し、テナント アカウントにアクセスするために必要なすべての権限を Cisco Cloud APIC に付与するには、テナント アカウントでテナント ロール cloud-formation テンプレートを実行します。このテンプレートは、インフラ テナントの AWS アカウントの capic-common-[capicAccountId]-data という名前の S3 バケットの tenant-cft.json オブジェクトとして使用できます。セキュリティ上の理由から、S3 バケットへのパブリック アクセスは許可されていないため、S3 バケット所有者はこのファイルをダウンロードしてテナント アカウントで使用する必要があります。
- 信頼されていないテナント：アカウント アクセスと秘密鍵を使用します。使用されるアクセス鍵と秘密鍵は、少なくともこれらのアクセス許可を持つ IAM ユーザーのものである必要があります。作成された IAM ロールは、`ApicTenantRole` という名前にする必要があります。

（注） Cloud APIC は、他のアプリケーションまたはユーザーによって作成された AWS リソースを妨害しません。自身で作成した AWS リソースのみを管理します。

```
{
    "Version": "2012-10-17",
    "Statement": [
       {
            "Action": [
                "ec2:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:*"
            ],
            "Resource": "*",
```

```
            "Effect": "Allow"
        }, {
            "Action": [
                "events:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "logs:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "cloudtrail:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "cloudwatch:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "resource-groups:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "sqs:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": "elasticloadbalancing:*",
            "Resource": "*",
           "Effect": "Allow"
        }, {
            "Action": [
                "config:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::<account-id>:role/ApicTenantRole",
            "Effect": "Allow"
        }
    ]
}
```

- 信頼関係の追加:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
           "Effect": "Allow",
           "Principal": {
               "Service": "vpc-flow-logs.amazonaws.com",
```

```
                "AWS": "arn:aws:iam::<account-d>:root"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

- Cloud APIC は所有権チェックを適用して、意図的にまたは誤って行われた同じテナントとリージョンの組み合わせでポリシーが展開されないようにします。たとえば、リージョン R1 の AWS アカウント IA1 に Cloud APIC が展開されているとします。ここで、リージョン R2 にテナント TA1 を展開します。このテナント展開（TA1-R2 のアカウントとリージョンの組み合わせ）は、IA1-R1 によって所有されています。別の Cloud APIC が将来のある時点で同じテナントとリージョンの組み合わせを管理しようとした場合（たとえば、CAPIC2 がリージョン R3 の AWS アカウント IA2 に導入されている場合）、これは展開 TA1-R2 の所有者が現在、IA1-R1 であるため許可されません。つまり、1 つの Cloud APIC で管理できるのは 1 つのリージョン内の 1 つのアカウントのみです。以下の例は、いくつかの有効な展開の組み合わせと間違った展開の組み合わせを示しています。

```
Capic1:
IA1-R1: TA1-R1 - ok
        TA1-R2 - ok

Capic2:
IA1-R2: TA1-R1 - not allowed
        TA1-R3 - ok

Capic3:
IA2-R1: TA1-R1 - not allowed
        TA1-R4 - ok
        TA2-R4 - ok
```

- 所有権の強制は、AWS リソース グループを使用して行われます。リージョン R2 のアカウント TA1 の新しいテナントが Cloud APIC によって管理される場合、リソース グループ CAPIC_TA1_R2 (例: CAPIC_123456789012_us-east-2) がテナント アカウントに作成されます。このリソース グループには、値が IA1_R1_TA1_R2 のリソース タグ AciOwnerTag があります (アカウント IA1 の Cloud APIC によって管理され、リージョン R1 に展開されていると想定)。AciOwnerTag の不一致が発生した場合、テナントとリージョンの管理は中止されます。

  AciOwnerTag の不一致ケースの概要は次のとおりです。

  - 最初に Cloud APIC がアカウントにインストールされ、次に削除され、Cloud APIC が別のアカウントにインストールされます。既存のすべてのテナント リージョンの展開が失敗します。
  - 別の TA1-R2 が同じテナント リージョンを管理しています。

  所有権が一致しない場合、**再試行** (テナント リージョンの再セットアップ) は現在サポートされていません。回避策として、他の CloudAPIC が同じテナントとリージョンの組み合わせを管理していないことが確実な場合は、テナントの AWS アカウントにログオンし、影響を受けるリソース グループ（CAPIC_123456789012_us-east-2など）を手動で削除します。次に、Cloud APIC をリロードするか、テナントを再度削除して追加します。

**ステップ 1** Cloud APIC で、AWS プロバイダーを作成します。

a) **[インテント（Intent）]** メニューで、ドロップダウンから **[テナント（tenant）]** > ***[tenant_name]*** を選択します。

b) **[インテント（Intent）]** ペインで、**[アプリケーション管理（Application Management）]** > ***[tenant_name]*** を選択します。

**ステップ 2** 次のアクションを実行します。

a) **[信頼された]** テナント チェックボックスがオンになっていることを確認します。

AWS アカウントは、クラウドを使用するユーザーテナントの信頼できるアカウントである必要があります。

b) **[クラウド アカウント ID]** フィールドで、クラウド アカウント ID を指定します。

c) インフラ テナントの AWS アカウントの s3 バケットにある URL https://capic-common-<infraAccountId>-data.s3.amazonaws.com/tenant-cft.json にあるテナント ロールの cloud-formation テンプレートを実行します。

（注） または、信頼済みフラグをオフのままにして、テナントに対して通常行われるようにアクセス鍵と秘密鍵を提供します。

**ステップ 3** [保存（Save）] をクリックします。

# リリース 4.2(3) 以降のテナント AWS プロバイダーの設定

### 始める前に

- AWS プロバイダーは、インフラ テナント用に自動設定されます。インフラ テナント用に AWS プロバイダーを構成するために何もする必要はありません。
- すべての非インフラ テナントの場合、AWS プロバイダーは、信頼できるテナント、信頼できないテナント、または組織のテナントとして設定されます。資格情報の管理は簡単ではないため、信頼できるテナントを使用することをお勧めします。また、各テナントは個別の AWS アカウントに属している必要があります。複数のテナントで同じ AWS アカウントを共有することは許可されていません。

  信頼できるテナントの場合、最初に Cisco Cloud APIC が展開されているアカウント (インフラ テナントのアカウント) との信頼関係を確立します。信頼関係を確立し、テナント アカウントにアクセスするために必要なすべての権限を Cisco Cloud APIC に付与するには、最初にテナントを作成し、そのテナントにアクセス タイプとして信頼済みタグを割り当てます。次に、[テナント]ページでテナント名をクリックして、その新しい信頼できるテナントを再度表示し、テナント ウィンドウの [AWS アカウント] 領域で、[CloudFormation テンプレートの実行] リンクをクリックします。
- 組織テナントは、組織の一部であるテナント アカウントを追加するためのものです。これには、組織のマスター アカウントに Cisco Cloud APIC を展開する必要があります。

- 信頼されていないテナントは、アカウントアクセスと秘密鍵を使用します。使用されるアクセス鍵と秘密鍵は、少なくともこれらのアクセス許可を持つ IAM ユーザーのものである必要があります。作成された IAM ロールは、`ApicTenantRole` という名前にする必要があります。

（注） Cloud APIC は、他のアプリケーションまたはユーザーによって作成された AWS リソースを妨害しません。自身で作成した AWS リソースのみを管理します。

```
{
    "Version": "2012-10-17",
    "Statement": [
       {
            "Action": [
                "ec2:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "events:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "logs:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "cloudtrail:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "cloudwatch:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "resource-groups:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": [
                "sqs:*"
            ],
```

```
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": "elasticloadbalancing:*",
            "Resource": "*",
           "Effect": "Allow"
        }, {
            "Action": [
                "config:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }, {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::<account-id>:role/ApicTenantRole",
            "Effect": "Allow"
        }
    ]
}
```

- 信頼関係の追加:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
           "Effect": "Allow",
           "Principal": {
               "Service": "vpc-flow-logs.amazonaws.com",
               "AWS": "arn:aws:iam::<infra-account-id>:root"
           },
           "Action": "sts:AssumeRole"
      }
   ]
}
```

- Cloud APIC は、AWS Organizations テナントのポリシーを管理するために、OrganizationAccountAccessRole IAM ロールを使用します。
  - マスター アカウント内の既存の組織内で AWS アカウントを作成した場合は、その作成した AWS アカウントに組織の OrganizationAccountAccessRole IAM ロールが自動的に割り当てられます。この場合、AWS のOrganizationAccountAccessRole の IAM ロールを手動で設定する必要はありません。
  - マスター アカウントが組織に参加するために既存の AWS アカウントを招待した場合は、AWS でOrganizationAccountAccessRole IAM ロールを手動で設定する必要があります。組織テナントの AWS で OrganizationAccountAccessRole IAM ロールを設定し、Cloud APIC に関連する権限があることを確認します。

    OrganizationAccountAccessRole IAM ロールは、組織またはアカウントに使用される SCP (サービス制御ポリシー) とともに、組織またはアカウントに対して、組織またはアカウントに使用する SCP (サービス制御ポリシー) とともに、組織のポリシーを管理するために Cloud APIC に必要な最小限の権限が付与されている必要があります。アクセス ポリシーの要件は、信頼できるテナントまたは信頼できないテナントの要件と同じです。

    ```
    {
        "Version": "2012-10-17",
        "Statement": [
    ```

```
{
     "Action": [
         "ec2:*"
     ],
     "Resource": "*",
     "Effect": "Allow"
 }, {
     "Action": [
         "s3:*"
     ],
     "Resource": "*",
     "Effect": "Allow"
 }, {
     "Action": [
         "events:*"
     ],
     "Resource": "*",
     "Effect": "Allow"
 }, {
     "Action": [
         "logs:*"
     ],
     "Resource": "*",
     "Effect": "Allow"
 }, {
     "Action": [
         "cloudtrail:*"
     ],
     "Resource": "*",
     "Effect": "Allow"
 }, {
     "Action": [
         "cloudwatch:*"
     ],
     "Resource": "*",
     "Effect": "Allow"
 }, {
     "Action": [
         "resource-groups:*"
     ],
     "Resource": "*",
     "Effect": "Allow"
 }, {
     "Action": [
         "sqs:*"
     ],
     "Resource": "*",
     "Effect": "Allow"
 }, {
     "Action": "elasticloadbalancing:*",
     "Resource": "*",
    "Effect": "Allow"
 }, {
     "Action": [
         "config:*"
     ],
     "Resource": "*",
     "Effect": "Allow"
 }, {
    "Action": "iam:PassRole",
    "Resource": "*",
    "Effect": "Allow"
   }
```

```
        ]
    }
```

組織テナントの信頼関係を追加するには:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
           "Effect": "Allow",
           "Principal": {
               "Service": "vpc-flow-logs.amazonaws.com",
               "AWS": "arn:aws:iam::<infra-account-id>:root"
           },
           "Action": "sts:AssumeRole"
      }
   ]
}
```

- Cloud APIC は所有権チェックを適用して、意図的にまたは誤って行われた同じテナントとリージョンの組み合わせでポリシーが展開されないようにします。たとえば、リージョン R1 の AWS アカウント IA1 に Cloud APIC が展開されているとします。ここで、リージョン R2 にテナント TA1 を展開します。このテナント展開（TA1-R2 のアカウントとリージョンの組み合わせ）は、IA1-R1 によって所有されています。別の Cloud APIC が将来のある時点で同じテナントとリージョンの組み合わせを管理しようとした場合（たとえば、CAPIC2 がリージョン R3 の AWS アカウント IA2 に導入されている場合）、これは展開 TA1-R2 の所有者が現在、IA1-R1 であるため許可されません。つまり、1 つの Cloud APIC で管理できるのは 1 つのリージョン内の 1 つのアカウントのみです。以下の例は、いくつかの有効な展開の組み合わせと間違った展開の組み合わせを示しています。

```
Capic1:
IA1-R1: TA1-R1 - ok
        TA1-R2 - ok

Capic2:
IA1-R2: TA1-R1 - not allowed
        TA1-R3 - ok

Capic3:
IA2-R1: TA1-R1 - not allowed
        TA1-R4 - ok
        TA2-R4 - ok
```

- 所有権の強制は、AWS リソース グループを使用して行われます。リージョン R2 のアカウント TA1 の新しいテナントが Cloud APIC によって管理される場合、リソース グループ CAPIC_TA1_R2 (例: CAPIC_123456789012_us-east-2) がテナント アカウントに作成されます。このリソース グループには、値が IA1_R1_TA1_R2 のリソース タグ AciOwnerTag があります (アカウント IA1 の Cloud APIC によって管理され、リージョン R1 に展開されていると想定)。AciOwnerTag の不一致が発生した場合、テナントとリージョンの管理は中止されます。

  AciOwnerTag の不一致ケースの概要は次のとおりです。

  - 最初に Cloud APIC がアカウントにインストールされ、次に削除され、Cloud APIC が別のアカウントにインストールされます。既存のすべてのテナント リージョンの展開が失敗します。

• 別の TA1-R2 が同じテナント リージョンを管理しています。

所有権が一致しない場合、**再試行** (テナント リージョンの再セットアップ) は現在サポートされていません。回避策として、他のCloudAPICが同じテナントとリージョンの組み合わせを管理していないことが確実な場合は、テナントの AWS アカウントにログオンし、影響を受けるリソース グループ（CAPIC_123456789012_us-east-2など）を手動で削除します。次に、Cloud APIC をリロードするか、テナントを再度削除して追加します。

**ステップ 1** Cloud APIC で、AWS プロバイダーを作成します。

a) **[インテント（Intent）]** メニューで、ドロップダウンから **[テナント（tenant）]** > ***[tenant_name]*** を選択します。

b) **[インテント（Intent）]** ペインで、**[アプリケーション管理（Application Management）]** > ***[tenant_name]*** を選択します。

**ステップ 2** 次のアクションを実行します。

a) **[AWS アカウント ID]** フィールドに、クラウド アカウント ID を指定します。

b) **[アクセス タイプ]** 領域で、**[信頼済み]** を選択します。

AWSアカウントは、クラウドを使用しているユーザーテナントの信頼できるアカウントである必要があります。

c) [保存（Save）] をクリックします。

d) **[テナント]** ページでテナント名をクリックして、新しい信頼できるテナントを再度表示します。

テナントの **[概要]** ページの **[AWS アカウント]** 領域に、次のメッセージが表示されます。「このテナントから設定をデプロイするには、AWSインフラアカウントとの信頼を確立する信頼できるロールをテナント AWS アカウントに作成する必要があります。これを行うには、以下のリンクを開いて CloudFormation テンプレートを実行してください」。

e) **[CloudFormation テンプレートの実行]** リンクをクリックします。

これにより、AWS サインイン ページに戻ります。このページには、Cloud APIC GUI のこれらの手順で前に入力した必要な AWS アカウント情報が事前に入力されているはずです。

f) サインイン情報が正しいことを確認したら、AWS サインイン ページで **[次へ]** をクリックします。

g) テナント アカウントでテナント ロールの cloud-formation テンプレートを実行します。

（注） または、信頼済みフラグをオフのままにして、テナントに対して通常行われるようにアクセス鍵と秘密鍵を提供します。

**ステップ 3** [保存（Save）] をクリックします。

# Cisco Cloud APIC GUI を使用したアプリケーション プロファイルの作成

このセクションでは、Cisco Cloud APIC GUI を使用したアプリケーション プロファイルの作成方法を説明します。

### 始める前に

テナントを作成します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

**[アプリケーション管理（Application Management）]** オプションのリストが **[インテント（Intent）]** メニューに表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[アプリケーション プロファイルの作成（Create Application Profile）]** をクリックします。**[アプリケーション プロファイルの作成（Create Application Profile）]** ダイアログ ボックスが表示されます。

**ステップ 4** [Name] フィールドに名前を入力します。

**ステップ 5** テナントを選択します。

a) **[テナントの選択（Select Tenant）]** をクリックします。

**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。

b) **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。

**[アプリケーションプロファイルの作成（Create Application Profile）]** ダイアログボックスで、次の手順を実行します。

**ステップ 6** **[説明（Description）]** フィールドに説明を入力します。

**ステップ 7** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用した VRF の作成

このセクションでは、Cisco Cloud APIC GUI を使用した VRF の作成方法について説明します。

### 始める前に

テナントを作成します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

**[アプリケーション管理（Application Management）]** オプションのリストが **[インテント（Intent）]** メニューに表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[VRF の作成（Create VRF）]** をクリックします。**[VRF の作成（Create VRF）]** ダイアログ ボックスが表示されます。

**ステップ 4** 次の *[VRF* ダイアログボックスの作成（*Create VRF*）*]* ダイアログボックスのフィールドの表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *3 : [VRF* の作成（*Create VRF*）*]* ダイアログボックスのフィールド

| **[プロパティ（Properties）]** | 説明 |
|---|---|
| 全般 | |
| 名前 | **[Name]** フィールドに、VRF の表示名を入力します。<br>すべての VRF に *vrfEncoded* 値が割り当てられます。テナントと VRF 名の組み合わせが 32 文字を超える場合、VRF 名（テナント名も含む）は *vrfEncoded* 値を使用してクラウド ルータで識別されます。*vrfEncoded* 値を表示するには、**[Application Management]** > **[VRFs]** サブタブに移動します。右側のペインで VRF をクリックし、クラウド ルータで *[Encoded VRF Name]* を探します。 |
| テナント | テナントを選択します。<br>1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。<br>2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[VRF の作成（Create VRF）]** ダイアログボックスに戻ります。 |
| 説明 | VRF の説明を入力します。 |
| 設定 > **IPv4 ユニキャスト アドレス ファミリ BGP ターゲット** | |

| [プロパティ（Properties）] | 説明 |
|---|---|
| フィルタの追加 | 1. 構成するユニキャスト アドレス ファミリ BGP ターゲットの **[ルート ターゲットの追加]** オプションをクリックします。<br>2. **[タイプ]** フィールドで次のオプションをクリックして選択します。<br>• **エクスポート**：ルート ターゲットを他の VRF にエクスポートできます<br>• **インポート**：ルート ターゲットは他の VRF からインポートされます<br>• **[ルート ターゲット]** テキスト ボックスに、現在の VRF からエクスポートまたは現在の VRF にインポートできるルート ターゲットを入力します。 |

**ステップ 5** 作業が完了したら、[保存（Save）] をクリックします。

# Cisco Cloud APIC GUI を使用した外部ネットワークの作成

この手順は、外部ポリシーの作成方法を示しています。オンプレミス サイトの複数のルータに接続できる単一の外部ネットワーク、または CCR への接続に使用できる複数の VRF を持つ複数の外部ネットワークを設定できます。

### 始める前に

外部ネットワークを作成する前に、ハブ ネットワークを作成しておく必要があります。

**ステップ 1** 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）]** > **[外部ネットワーク（External Networks）]** に移動します。
構成された外部ネットワークが表示されます。

**ステップ 2** **[アクション（Actions）]** をクリックし、**[外部ネットワークの作成（Create External Network）]** を選択します。
**[外部ネットワークの作成（Create External Network）]** ウィンドウが表示されます。

**ステップ 3** 次の *[外部ネットワークの作成ダイアログボックスのフィールド（Create External Network Dialog Box Fields）]* の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *4 : [*外部ネットワークの作成（***Create External Network***）*]* ダイアログボックスのフィールド

| **[プロパティ（Properties）]** | 説明 |
|---|---|
| 全般 | |
| 名前 | 外部ネットワーク名を入力します。 |
| **VRF** | この 外部VRF は、外部の非 ACI デバイスとの外部接続に使用されます。この目的で複数の 外部VRF を作成できます。<br>この VRF は、VRF が次の 3 つの特性をすべて備えている場合に 外部VRF として識別されます。<br>• インフラ テナントの下で構成された<br>• 外部ネットワークに関連付けられている<br>• クラウド コンテキスト プロファイルに関連付けられていない<br>外部ネットワークに関連付けられているVRFはすべて 外部VRF になります。外部VRF をクラウド コンテキスト プロファイルまたはサブネットに関連付けることはできません。<br>外部VRF を選択するには、次の手順を実行します。<br>1. **[VRF の選択（Select VRF）]** をクリックします。<br>**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。<br>2. **[VRFの選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択します。<br>[+ VRF の作成（+ Create VRF）] オプションを使用してVRFを作成することもできます。<br>3. [選択（Select）] をクリックします。<br>**[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。 |
| ルータ タイプ | ルータ タイプを選択します。<br>• **CCR**：<br>• 25.0(3) よりも前のリリースでは、シスコ クラウド サービス ルータ 1000V<br>• リリース 25.0(3) 以降では、Cisco Catalyst 8000V<br>• **TGW**: AWS トランジット ゲートウェイ ルーター |
| ホスト ルーター名 | このフィールドは、**[ルータ タイプ（Router Type）]** として **CCR** を選択した場合に表示されます。<br>このフィールドは編集できません。デフォルトのホスト ルータが自動的に選択されます。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| ハブ ネットワーク | このフィールドは、**ルータ タイプ**として **TGW** を選択した場合に表示されます。<br>ハブ ネットワークを選択するには:<br>1. **[ハブ ネットワークの選択]** をクリックします。<br>**[ハブ ネットワークの選択]** ダイアログボックスが表示されます。<br>2. **[ハブ ネットワークの選択]** ダイアログ ボックスで、リストから目的のハブ ネットワークをクリックし、**[選択]** をクリックします。<br>**[外部ネットワークの作成（Create External Network）]** ページに戻ります。 |
| 設定 | |
| 地域 | リージョンを選択するには:<br>1. **[地域の追加（Add Region）]** をクリックします。<br>**[地域の選択（Select Regions）]** ダイアログボックスが表示されます。<br>初回セットアップの一部として選択した地域がここに表示されます。<br>2. **[地域の選択（Select Regions）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。<br>**[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。 |

| [プロパティ（**Properties**）] | 説明 |
| --- | --- |
| **VPN** ネットワーク | |

| [プロパティ（Properties）] | 説明 |
|---|---|
| | VPN ネットワーク エントリは、外部接続に使用されます。設定されたすべてのVPNネットワークが、選択したすべてのリージョンに適用されます。<br>VPN ネットワークを追加するには、次の手順を実行します。<br>1. **[VPNネットワークの追加（Add VPN Network）]** をタップします。<br>**[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスが表示されます。<br>2. **[名前（Name）]** フィールドに VPN ネットワークの名前を入力します。<br>3. **[+ IPSec ピアの追加（+ Add IPSec Peer）]** をクリックします。<br>**[IPSec トンネル接続先の追加（Add IPSec Tunnel Destination）]** ウィンドウが表示されます。<br>4. 追加する IPSec トンネル接続先の次の次のフィールドに値を入力します。<br>• **IPSec トンネル ピアの パブリック IP**<br>• **事前共有キー**<br>• **IKE バージョン**: IPSec トンネル接続用に **ikev1** または **ikev2** を選択します。<br>• **BGP ピア ASN**<br>• **Subnet Pool Name**：**[サブネット プール名の選択（Select Subnet Pool Name）]** をクリックします。<br>**[サブネット プール名の選択（Select Subnet Pool Name）]** ダイアログボックスが表示されます。リストされている使用可能なサブネット プールのいずれかを選択し、**[選択（Select）]** をクリックします。<br>• **IPsec トンネル ソース インターフェイス**: このフィールドのエントリを使用して、Cisco Cloud APIC は、選択された各ソース インターフェイスから接続先 IP アドレスへの 1 つの IPsec トンネルを作成します。<br>（注） **ikev2** は、このフィールドのデフォルト オプションです。IPsec トンネル ソース インターフェイス機能は、IKEv2 構成でのみサポートされます。<br>**gig3**は、デフォルトで選択されます。次の中から1つまたは複数のインターフェイスを選択します<br>• **gig2**: GigabitEthernet2 インターフェイス<br>• **gig3**: GigabitEthernet3 インターフェイス<br>• **gig4**: GigabitEthernet4 インターフェイス<br>（注） この外部ネットワークで IPsec トンネル ソース インターフェイスを構成した後、ルーティング ポリシー: リリース 25.0(2)で説明されているように、 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| | 同じ接続先へのトンネルを形成できる追加のネットワークでIPsec トンネル ソース インターフェイスを構成できます。<br><br>5. **[追加（Add）]** をクリックして、この IPsec 接続先を追加します。<br>**[VPN ネットワークの追加]** ウィンドウに戻ります。<br>別の IPSec トンネル接続先を追加する場合は、**[+ IPSec ピアの追加（+ Add IPSec Peer）]** をクリックします。<br>6. **[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスで **[追加（Add）]** をクリックします。<br>**[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。 |

**ステップ 4** 外部ネットワークの作成が完了したら、**[保存（Save）]** をクリックします。
**[外部ネットワークの作成（Create External Network）]** ウィンドウで **[保存（Save）]** をクリックすると、クラウド ルータが AWS で構成されます。

# グローバル VRF 間ルート リーク ポリシーの構成

グローバル VRF 間ルート リーク ポリシー機能は、リリース 25.0(2) で導入されました。

始める前に

**[クラウド APIC セットアップ（Cloud APIC Setup）]** ウィンドウの **[コントラクト ベース ルーティング（Contract Based Routing）]** 領域で変更を行う前に、 グローバルな Inter-VRF ルート リーク ポリシーで提供された情報を確認してください。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[構成（Configuration）]** を選択します。

オプションのリストが **[インテント（Intent）]** メニューに表示されます。

**ステップ 3** **[インテント（Intent）]**メニューの **[構成（Configuration）]** リストで、**[クラウド APIC セットアップ（Cloud APIC Setup）]** をクリックします。
**[セットアップ - 概要]** ダイアログ ボックスが表示されます。

**ステップ 4** **[コントラクト ベースのルーティング]** 領域で、**[コントラクト ベースのルーティング]** フィールドの現在の設定を書き留めます。

**[コントラクト ベースのルーティング]**設定は、現在の内部VRFルート リーク ポリシーを反映しています。これは、インフラ テナントの下のグローバル ポリシーであり、ブール フラグを使用して、コントラクトがルート マップがない場合にルートを駆動できるかどうかを示します。

- **オフ**: デフォルト設定。ルートがコントラクトに基づいてリークされておらず、代わりにルート マップに基づいてリークされていることを示します。
- **オン（On）**: ルート マップが存在しない場合に、契約に基づいてルートが漏洩していることを示します。有効にすると、ルート マップが構成されていないときにコントラクトがルーティングを駆動します。ルート マップが存在する場合、ルート マップは常にルーティングを駆動します。

**ステップ 5** **[コントラクト ベースのルーティング]** フィールドの現在の設定を変更するかどうかを決定します。

ある設定から別の設定に切り替える場合は、次の手順に従います。

- **オン設定からオフへの切り替え (コントラクト ベースのルーティングを無効にする)**: この状況では、現在、コントラクト ベースのルーティングが構成されており、ルート マップベースのルーティングに切り替えることが想定されています。コントラクトベースのルーティングからルート マップベースのルーティングに切り替える前にルートマップ ベースのルーティングが設定されていない場合、これは混乱を招く可能性があります。

  この状況で**オン**設定から**オフ**設定に切り替える前に、次の変更を行います。

  1. 既存のコントラクトを持つ VRF のすべてのペア間で、ルート マップ ベースのルート リークを有効にします。

     Cisco Cloud APIC GUI を使用したリーク ルートの構成 （22 ページ） の手順を実行します。

  2. グローバル ポリシーでコントラクト ベースのルート ポリシーを無効にします。

     **[コントラクト ベースのルーティング]** フィールドのスイッチを **[オン]** 設定から **[オフ]** 設定に切り替えて、契約ベースのルーティングからルート マップ ベースのルーティングに切り替えます。

  3. 有効にした新しいルート マップ ベースのルーティングに基づいて必要な粒度を反映するようにルーティングを変更します。

- **オフ設定からオンへの切り替え (契約ベースのルーティングを有効にする)**: この状況では、現在ルートマップ ベースのルーティングが構成されており、契約ベースのルーティングに切り替えることが想定されています。コントラクトとルート マップの両方を VRF のペア間で有効にできるため、これは中断を伴う操作ではなく、付加的な操作です。このような状況では、ルーティングを有効にするときに、コントラクトよりもルート マップが優先されます。ルート マップ ベースのルーティングが有効になっている場合、コントラクト ベースのルーティングを追加しても中断は発生しません。

  そのため、この状況では、**オフ**設定から**オン**設定に切り替える前に変更を行う必要はありません。ただし、VRF のペア間でコントラクトとルート マップの両方を有効にせず、完全にコントラクト ベース ルーティングに移行する場合は、VRF 間のコントラクトを完全に設定し、**[コントラクト ベースのルーティング]** フィールドで **[オン]** 設定に切り替える前に VRF 間のルート マップを削除する必要があります。

**ステップ 6** **[コントラクト ベースのルーティング]** 領域の現在の設定を変更する場合は、必要なルーティングのタイプに基づいて設定を切り替えます。

**ステップ 7** **Cloud APIC セットアップ**の構成が完了したら、**[完了]** をクリックします。

# Cisco Cloud APIC GUI を使用したリーク ルートの構成

Cisco Cloud APIC GUI を使用してリーク ルートを設定する手順は、リリースによって若干異なります。

- 25.0(2) より前のリリースでは、独立したルーティング ポリシーを設定して、外部接続機能を使用して ACI クラウド サイトと外部宛先の間のルーティングを設定するときに、内部 VRF と外部 VRF の間でリークするルートを指定できます。これらの手順については、Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定 （22 ページ） を参照してください。
- リリース 25.0(2) 以降では、内部 VRF のペア間のルート マップベースのルート リークがサポートされています。これらの手順については、Cisco Cloud APIC GUI を使用した内部 VRF のリーク ルートの構成 （25 ページ） を参照してください。

## Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定

リーク ルートの設定は、ルーティング ポリシーとセキュリティ ポリシーが別々に設定されるリリース 25.0(1) アップデートの一部です。VRF 間ルーティングを使用すると、独立したルーティング ポリシーを設定して、外部接続機能を使用して ACI クラウド サイトと外部宛先との間のルーティングを設定するときに、内部 VRF と外部 VRF の間でリークするルートを指定できます。詳細については、「サポートされているルーティングとセキュリティ ポリシーの概要」を参照してください。

外部宛先は、AWS サイトと外部デバイスの間の接続の有効化 （28 ページ） 手順を使用して手動で構成する必要があります。外部の接続先は、別のクラウド サイト、ACI オンプレミス サイト、または分散拠点である可能性があります。

（注）
- これらの手順を使用して、リリース 25.0(1) で提供されたアップデートに基づいて、内部と 外部VRF の間でのみセキュリティ ポリシーに依存しないルーティング ポリシーを設定します。
- これらの手順を使用して、内部 VRF のペア間のルーティングを設定しないでください。その場合、リリース 25.0(1) より前の通常どおりにコントラクトを使用します。

**ステップ 1** 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）]** > **[VRF]**に移動します。
設定された VRF が表示されます。

**ステップ 2** **[リーク ルート（Leak Routes）]** タブをクリックします。
すでに構成されているリーク ルートが表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックし、**[リーク ルートの作成（Create Leak Route）]** を選択します。**[リーク ルートの作成（Create a Leak Route）]** ウィンドウが表示されます。

**ステップ 4** 次の *[リーク ルートの作成ダイアログボックスのフィールド（Leak Routes Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

**表 *5:* リーク ルートの作成ダイアログボックスのフィールド（*Leak Routes Dailog Box Fields*）**

| **[プロパティ（Properties）]** | **説明** |
|---|---|
| **Source VRF** | 送信元 VRF を選択するには：<br>**1.** **[送信元 VRF の選択（Select Source VRF）]** をクリックします。<br>**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。<br>**2.** **[VRFの選択（Select VRF）]** ダイアログで、送信元 VRF に使用するために左側の列の VRF をクリックして選択してます。<br>送信元 VRF は、内部または 外部VRF であることに注意してください。<br>**3.** **[選択（Select）]** をクリックして、この送信元 VRF を選択します。<br>**[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。 |
| **宛先 VRF** | 宛先 VRF を選択するには、次の手順を実行します。<br>**1.** **[宛先の選択（Select destination）]** をクリックします。<br>**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。<br>**2.** **[VRFの選択（Select VRF）]** ダイアログで、宛先 VRF に使用するために左側の列の VRF をクリックして選択してます。<br>送信元 VRF も内部 VRF である場合、接続先 VRF を内部 VRF にすることはできないことに注意してください。<br>**3.** **[選択（Select）]** をクリックして、この宛先 VRF を選択します。<br>**[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| **Type** | 構成するリーク ルートのタイプを選択します。<br>• **すべてをリーク**: 接続元 VRF から接続先 VRF にリークするために、すべてのルートを構成することを選択します。<br>この場合、デフォルトでは、エントリ `0.0.0.0/0` がサブネット IP エリアに自動的に入力されます。<br>• **サブネット IP**：接続元VRFから接続先VRFまでのリークのルートとして特定のサブネット IP アドレスを設定する場合に選択します。**[サブネット IP（Subnet IP）]** ダイアログ ボックスが表示されます。<br>**[サブネット IP（Subnet IP）]** ボックスに、VRF 間のリークのルートとしてサブネット IP アドレスを入力します。 |

**ステップ 5** 作業が完了したら、[保存（Save）] をクリックします。
**[成功（Success）]** ウィンドウが表示されます。

**ステップ 6** 追加の VRF 間ルート リークを設定するかどうかを決定します。

- VRF のペア間でリークする別のルートを追加する場合は、**[成功（Success）]** ウィンドウで **[別のリーク ルートの追加（Add Another Leak Route）]** オプションをクリックします。

  **[リーク ルートの追加（Add Leak Route）]** ウィンドウに戻ります。VRF のペア間でリークする別のルートを設定するには、ステップ 4 （23 ページ）ーステップ 5 （24 ページ） を繰り返します。

- リバース ルートを追加する場合は、次のようにします。
  - 以前の設定の宛先 VRF が送信元 VRF になり、
  - 以前の設定の送信元 VRF が宛先 VRF になります。

  次に、**[成功（Success）]** ウィンドウで **[リバース リーク ルートの追加（Add Reverse Leak Route）]** オプションをクリックします。

  **[リーク ルートの追加（Add Leak Route）]** ウィンドウに戻ります。ステップ 4 （23 ページ）ーステップ 5 （24 ページ） を繰り返して別のルートを設定しますが、今度は次のようになります。
  - **[送信元 VRF（Source VRF）]** フィールドで、前の設定で宛先 VRF として選択したVRF を選択します。
  - **[宛先 VRF（Destination VRF）]** フィールドで、前の設定で送信元 VRF として選択した VRF を選択します。

**ステップ 7** リーク ルートの設定が完了したら、**[完了（Done）]** をクリックします。

メイン **VRF** ページの **[リーク ルート（Leak Routes）]**タブが再び表示され、新しく設定されたリーク ルートが表示されます。

**ステップ 8** 送信元または宛先VRFの詳細情報を取得したり、構成済みのリークルートを変更したりするには、メイン **[VRF]** ページの**[リーク ルート（Leak Routes）]** タブで [VRF] をダブルクリックします。
そのルート テーブルの **[概要（Overview）]** ページが表示されます。

**ステップ 9** [VRF] ページの上部にある **[アプリケーション管理（Application Management）]** タブをクリックし、左側のナビゲーションバーで**[リーク ルート（Leak Routes）]**タブをクリックします。
この特定の VRF に関連付けられているリーク ルートが表示されます。

**ステップ 10** 必要に応じて、この VRF に関連付けられた追加のリーク ルートを設定します。

- この VRF からリーク ルートを追加するには、**[アクション（Actions）]** をクリックし、**[<VRF_name> からリーク ルートを追加（Add Leak Route from <VRF_name>）]**を選択します。

  **[リーク ルートの追加（Add Leak Router）]** ウィンドウが表示されます。ステップ 4 （23 ページ）の情報を使用して、必要な情報を入力します。**送信元 VRF** のエントリは事前に選択されており、この状況では変更できないことに注意してください。

- この VRF にリークルートを追加するには、**[アクション（Actions）]** をクリックし、**[<VRF_name> にリーク ルートを追加（Add Leak Route to <VRF_name>）]**を選択します。

  **[リーク ルートの追加（Add Leak Router）]** ウィンドウが表示されます。ステップ 4 （23 ページ）の情報を使用して、必要な情報を入力します。**宛先 VRF** のエントリは事前に選択されており、この状況では変更できないことに注意してください。

### 次のタスク

これでルーティング ポリシーが構成されました。ルーティング ポリシーとセキュリティ ポリシーは別であるため、セキュリティ ポリシーを別個に構成する必要があります。

- Cisco Cloud APIC GUI を使用した EPG の作成 （32 ページ）: 次の手順を使用して、外部 EPG を作成します。
- Cisco Cloud APIC GUI を使用したコントラクトの作成 （39 ページ）: これらの手順を使用して、外部 EPG とクラウド EPG 間のコントラクトを作成します。

## Cisco Cloud APIC GUI を使用した内部 VRF のリーク ルートの構成

リリース 25.0(2) 以降、内部 VRF 間のルート リーク で説明されているように、内部 VRF のペア間のルートマップベースのルートリークがサポートされます。この機能は、リリース25.0(1)で提供されたルーティングとセキュリティの分割更新を拡張したもので、ルーティングとセキュリティ ポリシーが別々に設定されています。

**ステップ 1** 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）]** > **[VRF]**に移動します。
設定された VRF が表示されます。

**ステップ 2** **[リーク ルート（Leak Routes）]** タブをクリックします。
すでに構成されているリーク ルートが表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックし、**[リーク ルートの作成（Create Leak Route）]** を選択します。
**[リーク ルートの作成（Create a Leak Route）]** ウィンドウが表示されます。

**ステップ 4** 次の *[リーク ルートの作成ダイアログボックスのフィールド（Leak Routes Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

**表 *6*: リーク ルートの作成ダイアログボックスのフィールド（*Leak Routes Dailog Box Fields*）**

| **[プロパティ（Properties）]** | 説明 |
|---|---|
| **Source VRF** | 送信元 VRF を選択するには：<br>**1.** **[送信元 VRF の選択（Select Source VRF）]** をクリックします。<br>**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。<br>**2.** **[VRFの選択（Select VRF）]** ダイアログで、送信元 VRF に使用するために左側の列の VRF をクリックして選択してます。<br>この手順は、内部 VRF のペア間のルート マップ ベースのルート リークのためのものであるため、接続元 VRF には内部 VRF を選択します。<br>**3.** **[選択（Select）]** をクリックして、この送信元 VRF を選択します。<br>**[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。 |
| **宛先 VRF** | 宛先 VRF を選択するには、次の手順を実行します。<br>**1.** **[宛先の選択（Select destination）]** をクリックします。<br>**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。<br>**2.** **[VRFの選択（Select VRF）]** ダイアログで、宛先 VRF に使用するために左側の列の VRF をクリックして選択してます。<br>この手順は、内部 VRF のペア間のルート マップ ベースのルート リークのためのものであるため、接続先 VRF には内部 VRF を選択します。<br>**3.** **[選択（Select）]** をクリックして、この宛先 VRF を選択します。<br>**[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| **Type** | 構成するリーク ルートのタイプを選択します。<br>• **すべてをリーク**: 接続元 VRF から接続先 VRF にリークするために、すべてのルートを構成することを選択します。<br>この場合、デフォルトでは、エントリ `0.0.0.0/0` がサブネット IP エリアに自動的に入力されます。<br>• **サブネット IP**：接続元VRFから接続先VRFまでのリークのルートとして特定のサブネット IP アドレスを設定する場合に選択します。**[サブネット IP（Subnet IP）]** ダイアログ ボックスが表示されます。<br>**[サブネット IP（Subnet IP）]** ボックスに、VRF 間のリークのルートとしてサブネット IP アドレスを入力します。 |

**ステップ 5** 作業が完了したら、[保存（Save）] をクリックします。
**[成功（Success）]** ウィンドウが表示されます。

**ステップ 6** 追加の VRF 間ルート リークを設定するかどうかを決定します。

- VRF のペア間でリークする別のルートを追加する場合は、**[成功（Success）]** ウィンドウで **[別のリーク ルートの追加（Add Another Leak Route）]** オプションをクリックします。

  **[リーク ルートの追加（Add Leak Route）]** ウィンドウに戻ります。VRF のペア間でリークする別のルートを設定するには、ステップ 4 （26 ページ）ーステップ 5 （27 ページ） を繰り返します。

- リバース ルートを追加する場合は、次のようにします。
  - 以前の設定の宛先 VRF が送信元 VRF になり、
  - 以前の設定の送信元 VRF が宛先 VRF になります。

  次に、**[成功（Success）]** ウィンドウで **[リバース リーク ルートの追加（Add Reverse Leak Route）]** オプションをクリックします。

  **[リーク ルートの追加（Add Leak Route）]** ウィンドウに戻ります。ステップ 4 （26 ページ）ーステップ 5 （27 ページ） を繰り返して別のルートを設定しますが、今度は次のようになります。
  - **[送信元 VRF（Source VRF）]** フィールドで、前の設定で宛先 VRF として選択したVRF を選択します。
  - **[宛先 VRF（Destination VRF）]** フィールドで、前の設定で送信元 VRF として選択した VRF を選択します。

**ステップ 7** リーク ルートの設定が完了したら、**[完了（Done）]** をクリックします。

メイン **VRF** ページの **[リーク ルート（Leak Routes）]**タブが再び表示され、新しく設定されたリーク ルートが表示されます。

**ステップ 8** 送信元または宛先VRFの詳細情報を取得したり、構成済みのリークルートを変更したりするには、メイン **[VRF]** ページの**[リーク ルート（Leak Routes）]** タブで [VRF] をダブルクリックします。
そのルート テーブルの **[概要（Overview）]** ページが表示されます。

**ステップ 9** [VRF] ページの上部にある **[アプリケーション管理（Application Management）]** タブをクリックし、左側のナビゲーションバーで**[リーク ルート（Leak Routes）]**タブをクリックします。
この特定の VRF に関連付けられているリーク ルートが表示されます。

**ステップ 10** 必要に応じて、この VRF に関連付けられた追加のリーク ルートを設定します。

- このVRFからリークルートを追加するには、**[アクション（Actions）]** をクリックし、**[<VRF_name> からリーク ルートを追加（Add Leak Route from <VRF_name>）]**を選択します。

  **[リーク ルートの追加（Add Leak Router）]** ウィンドウが表示されます。ステップ 4 （26 ページ）の情報を使用して、必要な情報を入力します。**送信元VRF**のエントリは事前に選択されており、この状況では変更できないことに注意してください。

- この VRF にリークルートを追加するには、**[アクション（Actions）]** をクリックし、**[<VRF_name> にリーク ルートを追加（Add Leak Route to <VRF_name>）]**を選択します。

  **[リーク ルートの追加（Add Leak Router）]** ウィンドウが表示されます。ステップ 4 （26 ページ）の情報を使用して、必要な情報を入力します。**宛先VRF**のエントリは事前に選択されており、この状況では変更できないことに注意してください。

# AWS サイトと外部デバイスの間の接続の有効化

次の手順に従って、インフラ VPC CCR から IPSec/BGP を使用して任意の外部デバイスへの IPv4 接続を手動で有効にします。

## 外部デバイス構成ファイルのダウンロード

**ステップ 1** Cisco Cloud APIC GUI で、**[ダッシュボード（Dashboard）]** をクリックします。
Cisco Cloud APIC の**ダッシュボード**が表示されます。

**ステップ 2** **[インフラストラクチャ]** > **[外部接続]**に移動します。
**[外部接続（External Connectivity）]** ウィンドウが表示されます。

**ステップ 3** **[アクション（Actions）]** > **[外部デバイス構成ファイルのダウンロード（Download External Device Configuration Files）]** をクリックします。
**[外部デバイス構成ファイルのダウンロード（Download External Device Configuration Files）]** ポップアップが表示されます。

**ステップ 4** ダウンロードする外部デバイス構成ファイルを選択し、**[ダウンロード（Download）]** をクリックします。
このアクションにより、CCR への IPv4 接続のための外部デバイスの手動構成に使用する構成情報を含む zip ファイルがダウンロードされます。

# AWS サイトと外部デバイスの間の接続の有効化

**ステップ 1** インフラ VPC CCR から EVPN を使用しない外部デバイスへの IPv4 接続を手動で有効にするために必要な情報を収集します。

**ステップ 2** 外部デバイスにログインします。

**ステップ 3** 外部ネットワーキング デバイスを接続するための構成情報を入力します。

外部デバイス構成ファイルのダウンロード （28 ページ） の手順を使用して外部デバイス構成ファイルをダウンロードした場合、最初のトンネルの構成情報を見つけて、その構成情報を入力します。

最初のトンネルの外部デバイス設定ファイルの例を示します。

```
! The following file contains configuration recommendation to connect an external networking device
 with the cloud ACI Fabric
! The configurations here are provided for an IOS-XE based device. The user is expected to understand
 the configs and make any necessary amends before using them
! on the external device. Cisco does not assume any responsibility for the correctness of the config.

! Tunnel to 128.107.72.122 1.100 [ikev2] for
hctunnIf.acct-[infra]/region-[westus]/context-[overlay-1]-addr-[10.115.9.128/25]/csr-[ct_routerp_westus_0:0]/tunn-34
! USER-DEFINED: please define gig-gateway: GIG-GATEWAY
! USER-DEFINED: please define GigabitEthernet2 if required
! USER-DEFINED: please define tunnel-id: 100 if required
! USER-DEFINED: please define vrf-name: infra:externalvrf1 if required
! USER-DEFINED: please define gig3-public-ip: 13.88.168.176 if 0.0.0.0 ip still not provided by AWS.
! Device:            128.107.72.122
! Tunnel ID:         100
! Tunnel counter:    1
! Tunnel address:    5.16.1.9
! Tunnel Dn:
acct-[infra]/region-[westus]/context-[overlay-1]-addr-[10.115.9.128/25]/csr-[ct_routerp_westus_0:0]/tunn-34
! VRF name:          infra:externalvrf1
! ikev:              ikev2
! Bgp Peer addr:     5.16.1.10
! Bgp Peer asn:      65015
! Gig3 Public ip:    13.88.168.176
! PreShared key:     device1azure
! ikev profile name: ikev2-100

vrf definition infra:externalvrf1
    rd 1:1

    address-family ipv4
        route-target export 64550:1
        route-target import 64550:1
    exit-address-family
exit

crypto ikev2 proposal ikev2-infra:externalvrf1
    encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
    integrity sha512 sha384 sha256 sha1
    group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-infra:externalvrf1
    proposal ikev2-infra:externalvrf1
exit

crypto ikev2 keyring keyring-ikev2-100
```

```
    peer peer-ikev2-keyring
        address 13.88.168.176
        pre-shared-key devicelazure
    exit
exit

crypto ikev2 profile ikev2-100
    match address local interface GigabitEthernet2
    match identity remote address 13.88.168.176 255.255.255.255
    identity local address 128.107.72.122
    authentication remote pre-share
    authentication local pre-share
    keyring local keyring-ikev2-100
    lifetime 3600
    dpd 10 5 on-demand
exit

crypto ipsec transform-set ikev2-100 esp-gcm 256
    mode tunnel
exit

crypto ipsec profile ikev2-100
    set transform-set ikev2-100
    set pfs group14
    set ikev2-profile ikev2-100
exit

interface Tunnel100
    vrf forwarding infra:externalvrf1
    ip address 5.16.1.10 255.255.255.252
    ip mtu 1400
    ip tcp adjust-mss 1400
    tunnel source GigabitEthernet2
    tunnel mode ipsec ipv4
    tunnel destination 13.88.168.176
    tunnel protection ipsec profile ikev2-100
exit

ip route 13.88.168.176 255.255.255.255 GigabitEthernet2 GIG-GATEWAY

router bgp 65015

address-family ipv4 vrf infra:externalvrf1
    redistribute connected
    maximum-paths eibgp 32

    neighbor 5.16.1.9 remote-as 65008
    neighbor 5.16.1.9 ebgp-multihop 255
    neighbor 5.16.1.9 activate
    neighbor 5.16.1.9 send-community both

    distance bgp 20 200 20
exit-address-family
```

次の図に、外部デバイス構成ファイルで使用される各フィールドセットの詳細を示します。

- 次の図に示すフィールドは、これらの領域の構成に使用されます。
  - vrf definition
  - IPSec global configurations

```
vrf definition Ext-V1
rd 1:10
!
address-family ipv4
  route-target export 64550:10
  route-target import 64550:10
!
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2
lifetime 28800
!
crypto isakmp keepalive 10 10 periodic
crypto isakmp aggressive-mode disable
!
```

VRF Definition

IPSec Global Configurations

- 次の図に示すフィールドは、これらの領域の構成に使用されます。
  - トンネルごとの IPSec および ikev1 構成
  - VRF ネイバーの BGP 設定

```
!
crypto keyring Ext-V1-1000-ike
  pre-shared-key address <50.18.55.126>[cAPIC CSR Gig3 public IP] key <abcdefg12345>
!
crypto isakmp profile Ext-V1-1000-ike
   keyring Ext-V1-1000-ike
   match identity address <50.18.55.126>[cAPIC CSR1 gig3 Public IP] 255.255.255.255
!
crypto ipsec transform-set Ext-V1-1000-ike esp-aes esp-sha-hmac
mode tunnel
!
crypto ipsec profile Ext-V1-1000-ike
set security-association lifetime kilobytes disable
set security-association replay window-size 512
set transform-set Ext-V1-1000-ike
set pfs group14
!
interface Tunnel1000
vrf forwarding Ext-V1
ip address 50.50.0.2[cAPIC CSR BGP Peer Addr] 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1400
tunnel source GigabitEthernet2
tunnel mode ipsec ipv4
tunnel destination <50.18.55.126>[cAPIC CSR1 gig3 Public IP]
tunnel protection ipsec profile Ext-V1-1000-ike
!
router bgp 64550
!
address-family ipv4 vrf Ext-V1
  redistribute connected
  neighbor <50.50.0.1>[cAPIC CSR1 Tunnel Inner IP Addr] remote-as 1234
  neighbor 50.50.0.1 ebgp-multihop 255
  neighbor 50.50.0.1 activate
  neighbor 50.50.0.1 send-community both
  neighbor <50.50.0.5>[cAPIC CSR1 Tunnel Inner IP Addr] remote-as 1234
  neighbor 50.50.0.5 ebgp-multihop 255
  neighbor 50.50.0.5 activate
  neighbor 50.50.0.5 send-community both
  distance bgp 20 200 20
!
ip route 50.18.55.126[cAPIC CSR1 gig3 Public IP] 255.255.255.255 GigabitEthernet2 10.10.0.103
```

IPSec and Ikev1
Per Tunnel Configurations

BGP Configurations for VRF Neighbor

- 次の図に示すフィールドは、これらの領域の構成に使用されます。
  - グローバル構成
  - トンネルごとの IPSec および ikev2 の構成

```
crypto ikev2 proposal ikev2-1
 encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
 integrity sha512 sha384 sha256 sha1
 group 24 21 20 19 16 15 14 2
!
crypto ikev2 policy ikev2-1
 proposal ikev2-1
!
crypto ikev2 keyring keyring-ikev2-2000
 peer peer-ikev2-keyring
  address 35.81.94.248 [cAPIC CSR1 gig3 Public IP]
  pre-shared-key abcdefg12345
!
crypto ikev2 profile ikev2-2000
 match address local interface GigabitEthernet3
 match identity remote address 35.81.94.248[cAPIC CSR1 gig3 Public IP] 255.255.255.255
 identity local address 52.53.49.193 [Local Device tunnel source interface Public IP (Gig3 public IP)]
 authentication remote pre-share
 authentication local pre-share
 keyring local keyring-ikev2-2000
 lifetime 3600
 dpd 10 5 on-demand
!
crypto ipsec transform-set ikev2-2000 esp-gcm 256
 mode tunnel
!
crypto ipsec profile ikev2-2000
 set transform-set ikev2-2000
 set pfs group14
 set ikev2-profile ikev2-2000
!
interface Tunnel2000
 vrf forwarding Ext-V1
 ip address 50.50.0.14 [cAPIC CSR1 BGP Peer Addr] 255.255.255.252
 ip mtu 1400
 ip tcp adjust-mss 1400
 tunnel source GigabitEthernet3
 tunnel mode ipsec ipv4
 tunnel destination 35.81.94.248[cAPIC CSR1 gig3 Public IP]
 tunnel protection ipsec profile ikev2-2000
```

Ikev2 Global Configurations

IPSec and Ikev2
Per Tunnel Configurations

**ステップ 4** 前の手順を繰り返して、追加のトンネルを構成します。

# Cisco Cloud APIC GUI を使用した EPG の作成

このセクションでは、Cisco Cloud APIC GUI を使用した EPG の作成方法を説明します。各サービスには、少なくとも 1 つのコンシューマ EPG と 1 つのプロバイダー EPG が必要です。

### 始める前に

アプリケーション プロファイルと VRF を作成します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

**[アプリケーション管理（Application Management）]** オプションのリストが **[インテント（Intent）]** メニューに表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[EPG の作成（Create EPG）]** をクリックします。**[EPG の作成（Create EPG）]** ダイアログ ボックスが表示されます。

**ステップ 4** 次の *[EPG* 作成ダイアログボックスのフィールド（*Create EPG Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *7 : [EPG* の作成（*Create EPG*）*]* ダイアログボックスのフィールド

| **[プロパティ（Properties）]** | 説明 |
|---|---|
| 名前（**Name**） | EPG の名前を入力します。 |
| テナント | テナントを選択します。<br>1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。<br>2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。 |
| アプリケーション プロファイル | アプリケーション プロファイルを選択します。<br>1. **[アプリケーション プロファイルの選択（Select Application Profile）]**をクリックします。**[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログ ボックスが表示されます。<br>2. **[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログで、左側の列のアプリケーションプロファイルをクリックして、**[選択]** をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。 |
| 説明 | EPG の説明を入力します。 |
| **[設定（Settings）]** | |
| タイプ（**Type**） | EPG タイプを選択します。<br>• **クラウド** - クリックして、クラウドに EPG を作成します。<br>• **外部** - クリックして外部 EPG を作成します。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| ルート到達可能性 | (外部 EPG の作成時に表示されます) **[ルート到達性（Route Reachability）]** ドロップダウン リストをクリックして、次を選択します。<br>• **オンプレミス**<br>• **インターネット**<br>• **[Unspecified]** |
| **VRF** | VRF を選択するには、次の手順を実行します。<br>1. **[VRF の選択（Select VRF）]** をクリックします。**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。<br>2. **[VRF の選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択し、**[選択（Select）]** をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。 |

| [プロパティ（**Properties**）] | 説明 |
| --- | --- |
| エンドポイントセレクタ | |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | （注） エンドポイント セレクタ構成プロセスの一部として AWS で仮想マシンを設定する手順については、AWS でのインスタンスの設定 （50 ページ） を参照してください。<br><br>エンドポイント セレクタを追加するには：<br><br>1. **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックして、**[エンドポイント セレクタの追加]** ダイアログを開きます。<br><br>2. **[エンドポイント セレクタの追加（Add Endpoint Selector）]** ダイアログの **[Name（名前）]** フィールドに名前を入力します。<br><br>3. **[セレクタ式（Selector Expression）]** をクリックします。**[キー（Key）]**、**[演算子（Operator）]**、および **[値（Value）]** フィールドが有効になります。<br><br>4. **[キー（Key）]** ドロップダウン リストをクリックしてキーを選択します。次のオプションがあります。<br><br>• エンドポイントセレクタに IP アドレスまたはサブネットを使用する場合は、**[IP]** を選択します。<br><br>• エンドポイント セレクタにアベイラビリティ ゾーンを使用する場合は、**[ゾーン]** を選択します。<br><br>• エンドポイント セレクタに Amazon Web Services リージョンを使用する場合は、**[リージョン（Region）]** を選択します。<br><br>• エンドポイントセレクタのカスタム キーを作成する場合は、**[カスタム（Custom）]** を選択します。<br><br>（注） **[カスタム（Custom）]** オプションを選択すると、ドロップダウン リストがテキスト ボックスになります。**custom:** の後にスペースのキーの名前を入力する必要があります（例：**custom: Location**）。 |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | 5. **[演算子（Operator）]** ドロップダウン リストから演算子を選択します。次のオプションがあります。<br>• **[等しい (Equals）]**: 値フィールドに 1 つの値がある場合に使用します。<br>• **[等しくない（Not Equals）]**: 値フィールドに 1 つの値がある場合に使用されます。<br>• **[の中にある（In）]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。<br>• **[の中にない（Not In）]**: 値フィールドに複数のカンマ区切り値がある場合に使用されます。<br>• **[キーを持つ（Has Key）]**: 式にキーのみが含まれている場合に使用されます。<br>• **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用されます。<br>6. **[値（Value）]** フィールドに値を入力し、チェックマークをクリックしてエントリを検証します。入力する値は、**[キー（Key）]** フィールドと **[演算子（Operator）]** フィールドで選択した内容によって異なります。たとえば、**[キー（Key）]** フィールドが **[IP]** に設定され、**[演算子（Operator）]** フィールドが **[等しい（equals）]** に設定されている場合、**[値（Value）]** フィールドはIP アドレスまたはサブネットでなければなりません。ただし、**[演算子（Operator）]** フィールドが **[キー（keys）]** に設定されている場合、**[値（Value）]** フィールドは無効になります。<br>7. 完了したら、チェックマークをクリックしてセレクタ式を検証します。 |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | **8.** エンドポイントセレクタに追加のエンドポイントセレクタ式を作成するかどうかを決定します。単一のエンドポイントセレクタで複数の式を作成した場合、それらの式の間には論理ANDがあるものとみなされます。<br><br>たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。<br><br>• エンドポイント セレクタ 1、式 1:<br>• **[キー (Key):]** Zone<br>• **演算子 (Operator）** : equals<br>• **[値 (Value):]** us-west-1a<br><br>• エンドポイント セレクタ1、式 2:<br>• **[キー (Key):]** IP<br>• **演算子 (Operator）** : equals<br>• **[値 (Value):]** 192.0.2.1/24<br><br>この場合、これらの式の両方が真になる場合(アベイラビリティ ゾーンが us-west-1a で、IP アドレスがサブネット 192.0.2.1/24 に属している場合) に、そのエンドポイントはクラウド EPG に割り当てられます。 |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | **9.** このエンドポイントセレクタで作成するすべての式を追加した後で、チェックマークをクリックし、終了したら、**[追加（Add）]** をクリックします。<br><br>EPGの下で複数のエンドポイントセレクタを作成した場合は、それらのエンドポイントセレクタの間には論理ORがあるものとみなされます。たとえば、前のステップで説明したようにエンドポイントセレクタ1を作成し、次に、次に示すように2番目のエンドポイントセレクタを作成したとします。<br><br>• エンドポイントセレクタ2、式1:<br>• **[キー (Key):]** Region<br>• **演算子**： in<br>• **[値 (Value):]** us-east-1a, us-east-2<br><br>その場合、次のようになります。<br><br>• アベイラビリティ ゾーンが us-west-1a で、IPアドレスが192.0.2.1/24サブネットに属している (エンドポイントセレクタ1の式)<br><br>または<br><br>• リージョンが us-east-1a または us-east-2 (エンドポイントセレクタ2の式) のいずれかである<br><br>その場合、エンドポイントがクラウドEPGに割り当てられます。 |

**ステップ5** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用したコントラクトの作成

このセクションでは、Cisco Cloud APIC GUI を使用したコントラクトの作成方法について説明します。

### 始める前に

フィルタを作成します。

**ステップ 1** インテント アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

**[アプリケーション管理（Application Management）]** オプションのリストが **[インテント（Intent）]** メニューに表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[コントラクトの作成（Create Contract）]** をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログ ボックスが表示されます。

**ステップ 4** 次の *[*コントラクト ダイアログ ボックス フィールドの作成（*Create Contract Dialog Box Fields*）*]* テーブルにリストされているように、各フィールドに適切な値を入力して続行します。

**表 *8 : [*コントラクトの作成（*Create Contract*）*]* ダイアログボックスのフィールド**

| **[プロパティ（Properties）]** | **説明** |
|---|---|
| **名前（Name）** | 契約の名前を入力します。 |
| **テナント** | テナントを選択します。<br>1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。<br>2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。 |
| **説明** | コントラクトの説明を入力してください。 |
| **[設定（Settings）]** | |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| スコープ | このスコープは、同じアプリケーションプロファイル内、同じVRFインスタンス内、ファブリック全体（グローバル）、または同じテナント内のエンドポイント グループにコントラクトを制限します。<br>（注） 共有サービスにより、異なるテナントのEPG間および異なるVRFのEPG間の通信が可能になります。<br>1つのテナントのEPGが別のテナントのEPGと通信できるようにするには、**[グローバル（Global）]** スコープを選択します。<br>1つのVRFのEPGが別のVRFの別のEPGと通信できるようにするには、**[グローバル（Global）]** または**[テナント（Tenant）]** スコープを選択します。<br>共有サービスの詳細については、共有サービス を参照してください。<br>ドロップダウン矢印をクリックして、次のスコープオプションから選択します。<br>• **アプリケーション プロファイル**<br>• **VRF**<br>• **Global**<br>• **テナント** |
| フィルタを両方向に適用 | チェックボックスをオンにして、コンシューマーからプロバイダーおよびプロバイダーからコンシューマーへのトラフィックに同じフィルターを適用します。トラフィックの方向ごとに異なるフィルタを適用する場合は、ボックスにチェックを入れないでください。<br>デフォルトでチェックボックスはオンになっています。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| フィルタの追加 | フィルタを選択します。<br>1. [フィルタの追加（Add Filter）] をクリックします。フィルタ行が表示され、**[フィルタの選択（Select Filter）]** オプションが表示されます。<br>2. **[フィルタの選択（Select Filter）]** をクリックします。**[フィルタの選択（Select Filter）]** ダイアログボックスが表示されます。<br>3. **[フィルタの選択（Select Filter）]** ダイアログで、左側の列のフィルタをクリックして選択し、**[選択（Select）]** をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。 |

**ステップ 5** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC を使用したコンシューマおよびプロバイダー EPG の指定

ここでは、EPGをコンシューマまたはプロバイダーとして指定する方法について説明します。

### 始める前に

- コントラクトを設定できます。
- EPG が設定済みです。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[構成（Configuration）]** を選択します。

**[インテント（Intent）] の [構成（Configuration）]** オプションのリストが表示されます。

**ステップ 3** **[インテント（Intent）]**メニューの **[構成（Configuration）]** リストで、**[EPG Communication]** をクリックします。**[EPG通信（EPG Communication）]** ダイアログボックスに、**コンシューマ EPG**、**コントラクト**、および**プロバイダー EPG**の情報が表示されます。

**ステップ 4** コントラクトを選択します。

a) **[コントラクトの選択（Select Contract）]** をクリックします。**[コントラクトの選択（Select Contract）]** ダイアログ ボックスが表示されます。

b) **[コントラクトの選択（Select Contract）]** ダイアログの左側のペインで、契約をクリックして選択し、**[選択（Select）]** をクリックします。**[コントラクトの選択（Select Contract）]** ダイアログ ボックスが閉じます。

**ステップ 5** コンシューマ EPG を追加するには、次の手順を実行します。

a) **[コンシューマ EPG の追加（Add Consumer EPGs）]** をクリックします。**[コンシューマー EPG の選択（Select Consumer EPGs）]** ダイアログが表示されます。

b) **[コンシューマー EPG の選択（Select Consumer EPGs）]** ダイアログの左側のペインで、チェックボックスをオンにして EPG を選択します。

**ステップ 6** プロバイダー EPG を追加するには、次の手順を実行します。

a) **[プロバイダー EPG の追加（Add Provider EPGs）]** をクリックします。**[プロバイダー EPG の選択（Select Provider EPGs）]** ダイアログが表示されます。

b) **[プロバイダーEPGの選択（Select Provider EPGs）]** ダイアログの左側のペインで、チェックボックスをオンにしてプロバイダー EPG を選択します。

c) 完了したら、**[選択（Select）]** をクリックします。**[プロバイダー EPG の選択（Select Provider EPGs）]** ダイアログボックスが閉じます。

# Cisco Cloud APIC GUI を使用したフィルタの作成

このセクションでは、クラウド APIC GUI を使用したフィルタの作成方法について説明します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

**[アプリケーション管理（Application Management）]** オプションのリストが**[インテント（Intent）]** メニューに表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[フィルタの作成（Create Fileter）]** をクリックします。**[フィルタの作成（Create Filter）]** ダイアログボックスが表示されます。

**ステップ 4** 次の *[フィルタの作成ダイアログボックスのフィールド（Create Filter Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

**表 *9*: フィルタの作成ダイアログボックスのフィールド**

| **[プロパティ（Properties）]** | 説明 |
|---|---|
| **名前（Name）** | **[名前（Name）]** フィールドにハードウェア フィルタの名前を入力します。 |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| テナント | テナントを選択します。<br>1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。<br>2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[フィルタの作成（Create ）]** ダイアログボックスに戻ります。 |
| 説明 | フィルタの説明を入力します。 |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| **Add Filter** | |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | フィルタを追加するには、次の手順を実行します。<br>1. **[フィルタ エントリの追加（Add Filter Entry）]** をクリックします。**[フィルタ エントリの作成（Create Filter Entry）]** ダイアログボックスが表示されます。<br>2. **[名前（Name）]** フィールドにフィルタエントリの名前を入力します。<br>3. **[フィルタの選択（Select Filter）]** ダイアログで、左側の列のフィルタをクリックして選択し、**[選択（Select）]** をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。<br>4. **[イーサネット タイプ（Ethernet Type）]** ドロップダウン リストをクリックして、イーサネットタイプを選択します。次のオプションがあります。<br>• **IP**<br>• **[Unspecified]**<br>（注） **[指定なし（Unspecified）]** を選択すると、残りのフィールドが無効になります。<br>5. **[IP プロトコル（IP Protocol）]** ドロップダウンメニューをクリックして、プロトコルを選択します。次のオプションがあります。<br>• **icmp**<br>• **tcp**<br>• **udp**<br>• **[Unspecified]**<br>（注） 残りのフィールドは、**tcp** または **udp** が選択されている場合にのみ有効になります。<br>6. **[送信元ポート（Origin Port）]** の **[開始]** と **[終了]** フィールドに適切なポート情報を入力します。<br>7. **[宛先ポート（Origin Port）]** の **[開始]** と **[終了]** |

| [プロパティ（Properties）] | 説明 |
|---|---|
| | フィールドに適切なポート情報を入力します。<br>8. フィルタ エントリ情報の入力が完了したら、**[追加（Add）]** をクリックします。**[フィルタの作成（Create Filter）]** ダイアログボックスに戻り、別のフィルタ エントリを追加する手順を繰り返すことができます。 |

**ステップ 5** 作業が完了したら、[保存（Save）] をクリックします。

# Cisco Cloud APIC GUI を使用したクラウド コンテキスト プロファイルの作成

このセクションでは、Cisco Cloud APIC GUI を使用したロールの作成方法について説明します。

### 始める前に

VRF を作成します。

**ステップ 1** **[アプリケーション管理（Application Management）]** > **[クラウド コンテキスト プロファイル（Cloud Context Profiles）]** に移動します。

構成されたクラウド コンテキスト プロファイルのリストが表示されます。

**ステップ 2** **[アクション（Actions）]** > **[クラウド コンテキスト プロファイル）Create Cloud Context Profile]** を順に選択します。

**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログ ボックスが表示されます。

**ステップ 3** 次の *[クラウド コントラクト プロファイルの作成ダイアログボックスのフィールド（Create Cloud Context Profile Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

**表 *10:* クラウド コントラクト プロファイルの作成ダイアログボックスのフィールド**

| [プロパティ（Properties）] | 説明 |
|---|---|
| 名前（Name） | クラウド コンテキスト プロファイルの名前を入力します。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| テナント | テナントを選択します。<br>1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。<br>2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスで、次の手順を実行します。 |
| 説明 | （オプション）クラウド コンテキスト プロファイルの説明を入力します。 |
| **[設定（Settings）]** | |
| 地域を選択 | リージョンを選択するには:<br>1. **[リージョンの選択（Select Region）]** をクリックします。**[リージョンの選択（Select Region）]** ダイアログボックスが表示されます。<br>2. **[リージョンの選択（Select Region）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスで、次の手順を実行します。 |
| **VRFの選択(Select VRF)** | VRF を選択するには、次の手順を実行します。<br>1. **[VRF の選択（Select VRF）]** をクリックします。**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。<br>2. **[VRF の選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスに戻ります。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| **CIDR の追加（Add CIDR）** | （注） 次のサブネットは予約済みであり、この **[CIDR の追加（Add CIDR）]** フィールドでは使用しないでください。<br>• 169.254.0.0/16（トランジット ゲートウェイへの VPN トンネル用に予約済み）<br>• 192.168.100.0/24（ブリッジ ドメイン インターフェイス用に CCR によって予約済み）<br><br>CIDR を追加するには、次の手順を実行します。<br>**1.** **[CIDR の追加（Add CIDR）]** をクリックします。**[CIDR の追加（Add CIDR）]** ダイアログボックスが表示されます。<br>**2.** **[アドレス（Address）]** フィールドに IP アドレスを入力します。<br>**3.** **[サブネットの追加（Add subnet）]** をクリックして、サブネット アドレスを **[アドレス（Address）]** に入力します。<br>**4.** アベイラビリティ ゾーンを追加するには:<br>**1.** **[アベイラビリティ ゾーンの選択（Select Availability Zone）]** を選択します。**[アベイラビリティ ゾーンの選択（Select Availability Zone）]** ダイアログボックスが表示されます。<br>**2.** **[アベイラビリティ ゾーンの選択]** ダイアログ ボックスで、左側の列でアベイラビリティ ゾーンをクリックして選択します。<br>リリース 25.0(2) 以降、このウィンドウに表示されるアベイラビリティ ゾーンのタイプは、このクラウド コンテキスト プロファイルに選択したテナントのタイプによって異なります。<br>（注） **ユーザー** テナントでクラウド コンテキスト プロファイルを作成している場合、このウィンドウでは **クラウド** アベイラビリティ ゾーンのみに制限されます。<br>詳細については、「可用性ゾーン」を参照してください。<br>**3.** [選択（Select）] をクリックします。<br>**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスに戻ります。<br>**5.** **[プライマリ（Primary）]** チェックボックスをオン（有効）またはオフ（無効）にします。<br>**6.** 完了したら、**[追加（Add）]** をクリックします。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| **VPNゲートウェイルータ** | (オプション) **VPN ゲートウェイ ルータ**のチェックボックスをクリックしてオン (有効) またはオフ (無効) にします。 |
| **TGW 添付ファイル** | (オプション) **TGW 添付ファイル**のチェックボックスをクリックしてオン (有効) またはオフ (無効) にします。 |

**ステップ 4** 設定が終わったら [Save] をクリックします。

# AWS でのインスタンスの設定

Cisco Cloud APIC のためのエンドポイント セレクタを設定するとき、Cisco Cloud APIC のために構成されたエンドポイント セレクタに対応する AWS で必要になるインスタンスを構成するためにも必要です。

このトピックでは、AWS でインスタンスを設定する手順について説明します。Cisco Cloud APIC のためのエンドポイント セレクタを設定する前に、または後で、これらの手順を使用して AWS のインスタンスを設定することができます。たとえば、先に AWS のアカウントに移動し、AWS のカスタム タグまたはラベルを作成してから、Cisco Cloud APIC のカスタム タグまたはラベルを使用して、エンドポイントセレクタを作成することができます。または、Cisco Cloud APIC でカスタムタグまたはラベルを使用してエンドポイントセレクタを作成してから、AWS のアカウントに移動し、AWS のカスタム タグまたはラベルを作成することもできます。

**ステップ 1** クラウドコンテキストプロファイルの設定を確認し、AWSインスタンスで使用する設定を決定します。

AWS インスタンスの構成プロセスの一環として、クラウド コンテキスト プロファイルを設定する必要があります。GUIを使用してクラウドコンテキストプロファイルを設定すると、VRFやリージョンの設定などの設定情報は、後で AWS にプッシュされます。

a) **[ナビゲーション (Navigation)]** メニューで、**[アプリケーション管理 (Application Management)]** タブを選択します。

**[アプリケーション管理 (Application Management)]** タブを展開すると、サブタブ オプションのリストが表示されます。

b) **[クラウド コンテキスト プロファイル (Cloud Context Profiles)]** サブタブ オプションを選択します。

Cisco Cloud APIC 用に作成したクラウド コンテキスト プロファイルのリストが表示されます。

c) この AWS インスタンス設定プロセスの一部として使用するクラウド コンテキスト プロファイルを選択します。

リージョン、VRF、IP アドレス、サブネットなど、このクラウド コンテキスト プロファイルのさまざまな設定パラメータが表示されます。AWS インスタンスを設定するときには、このウィンドウに表示される情報を使用します。

**ステップ 2** まだログインしていない場合は、 Cisco Cloud APICユーザテナントの Amazon Web Services アカウントにログインします。

**ステップ 3** **[サービス (Services)]** > **[EC2]** > **[インスタンス (Instances)]** > **[インスタンスの起動 (Launch Instance)]** に移動します。

**ステップ 4** **[Amazon マシン イメージ (AMI )の選択 (Choose Amazon Machine Image (AMI))]** ページで、Amazon マシン イメージ (AMI) を選択します。

**ステップ 5** **[インスタンス タイプの選択 (Choose An Instance type)]** ページで、インスタンス タイプを選択し、**[インスタンスの詳細の設定 (Configure instance Detail)]** をクリックします。

**ステップ 6** **[インスタンスの詳細の設定 (Configure instance Detail)]** ページで、該当するフィールドに必要な情報を入力します。

- **[ネットワーク (Network)]** フィールドで、Cisco Cloud APIC VRF を選択します。

  これは、この AWS インスタンス設定プロセスの一部として使用しているクラウド コンテキスト プロファイルに関連付けられている VRF です。

- **[サブネット (Subnet)]** フィールドに、サブネットを入力します。

- パブリック IP を使用する場合は、**[パブリック IP の自動割り当て (Auto Assign public IP)]** フィールドで、スクロールダウンメニューから **[有効 (Enable)]** を選択します。

**ステップ 7** **[インスタンスの詳細の設定 (Configure Instance Details)]** ページに必要な情報を入力したら、**[ストレージを追加 (Add Storage)]** をクリックします。

**ステップ 8** **[ストレージの追加 (Add Storage)]** ページで、デフォルト値を受け入れるか、必要に応じてこのページでストレージを設定し、**[タグの追加 (add Tags)]** をクリックします。

**ステップ 9** **[タグの追加 (Add Tags)]** ページで、**[タグの追加 (add Tag)]** をクリックし、このページの該当するフィールドに必要な情報を入力します。

（注） これらの手順の後の部分で、エンドポイントセレクタのタイプに対してIPアドレス、リージョン、またはゾーンを使用する場合は、このページに情報を入力する必要はありません。このような状況では、AWS でインスタンスを開始すると、Cisco Cloud APIC によって IP アドレス、リージョン、またはゾーンが検出され、エンドポイントが EPG に割り当てられます。

- **[キー (Key):]** これらの手順で後で追加するエンドポイント セレクタのタイプのカスタム タグを作成するときに使用するキーを入力します。

- **[値 (Value):]** このキーで使用する値を入力します。

- **[インスタンス (Instance):]** このフィールドのチェックボックスをオンにします。

- **[ボリューム (Volume):]**このフィールドのチェックボックスをオンにします。

たとえば、これらの手順で後ほど、エンドポイントセレクタの特定のビルディングのカスタム タグを作成する予定の場合 (building6 など) は、このページの次のフィールドに次の値を入力できます。

- **[キー (Key):]** ロケーション

- **[値 (value):]** building6

**ステップ 10** **[確認して起動する（Review and Launch）** をクリックします。

**既存のキー ペアを選択するか、新しいキー ペアを作成します。キーペアの** ページが表示されます。後ほどインスタンスに ssh 接続する場合は、このページの情報を使用します。

# Cisco Cloud APIC GUI を使用したバックアップ構成の作成

ここでは、バックアップ構成を作成する方法を説明します。

### 始める前に

必要に応じて、リモート ロケーションとスケジューラを作成します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[操作（Operations）]** を選択します。

**[インテント（Intent）]** の **[操作（Operations）]** オプションのリストが表示されます。

**ステップ 3** **[インテント（Intent）]** の **[操作（Operations）]** リストから、**[バックアップ構成の作成（Create Backup Configuration）]** をクリックします。**[バックアップ構成の作成（Create Backup Configuration）]** ダイアログ ボックスが表示されます。

**ステップ 4** 次の *[*バックアップ構成の作成ダイアログボックスのフィールド（*Create Backup Configuration Dialog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

**表 *11* : バックアップ構成の作成ダイアログボックスのフィールド**

| **[プロパティ（Properties）]** | 説明 |
|---|---|
| 全般 | |
| 名前 | バックアップ構成の名前を入力します。 |
| 説明 | バックアップ構成の説明を入力します。 |
| **Settings** | |
| **Backup Destination** | バックアップ接続先を選択します。<br>• **Local**<br>• **[リモート（Remote）]** |

| [プロパティ（**Properties**）] | 説明 |
| --- | --- |
| バックアップ オブジェクト | |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | バックアップで考慮するルート階層コンテンツを選択します<br>• ポリシー ユニバース<br>• セレクタオブジェクト（Selector Object）：これを選択すると、[オブジェクトタイプ（Object Type）] ドロップダウンリストと [オブジェクト DN（Object DN）] フィールドが追加されます。<br>1. オブジェクトタイプ（Object Type）ドロップダウン リストで、次のオプションから選択します。<br>• テナント（Tenant）：選択すると、[テナントの選択（Select Tenant）] オプションが表示されます。<br>• アプリケーション プロファイル（Application Profile）：選択すると、[アプリケーション プロファイルの選択（Select Application Profile）] オプションが表示されます。<br>• EPG：これを選択すると [EPG の選択（Select EPG）] オプションが表示されます。<br>• コントラクト（Contract）：これを選択すると、[コントラクトの選択（Select Contract）] オプションが表示されます。<br>• フィルタ（Filter）：これを選択すると、[フィルタの選択（Select Filter）] オプションが表示されます。<br>• VRF：これを選択すると、[VRFの選択（Select VRF）] オプションが表示されます。<br>• デバイス：[SelectfvcloudLBCtx] プションが表示されます。<br>• サービス グラフ：選択すると、[Select Service Graph] オプションが表示されます。<br>• [クラウド コンテキスト プロファイル（Cloud Context Profile）]：これを選 |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | 択すると、**[クラウド コンテキスト プロファイルの選択**（Select Cloud Context Profile）]オプションが表示されます。<br><br>2. **Select <object_name>** をクリックjします。**Select <object_name>** ダイアログが表示されます。<br><br>3. **Select <object_name>** ダイアログから左側の列のオプションからクリックして選んで、**[選択（Select）]** をクリックします。**[バックアップ構成の作成（Create Backup Configuration）]** ダイアログ ボックスに戻ります。<br><br>（注） **[オブジェクトDN（Object DN）]** フィールドには、バックアップするオブジェクトツリーのルートとして使用するオブジェクトの DN が自動的に入力されます。<br><br>• **DN の入力**（**Enter DN**）：このオプションを選択すると、**[オブジェクト DN（Object DN）]** フィールドが表示されます。<br><br>1. **[オブジェクトDN（Object DN）]** フィールドに、バックアップするオブジェクト ツリーのルートとして使用する特定のオブジェクトの DN を入力します。 |
| スケジューラ | 1. **[スケジューラの選択（Select Scheduler）]** をクリックして **[スケジューラの選択（Select Scheduler）]** ダイアログを開き、左側の列からスケジューラを選択します。<br><br>2. 終了したら、右下隅にある **[選択（Select）]** ボタンをクリックします。 |
| 作成後のバックアップのトリガー | 次のいずれかを選択します。<br><br>• **はい**（**Yes**）：（デフォルト）バックアップ設定の作成後にバックアップをトリガーします。<br><br>• **いいえ**（**No**）：バックアップ設定の作成後にバックアップをトリガーしません。 |

**ステップ 5** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用したテクニカル サポート ポリシーの作成

このセクションでは、テクニカル サポート ポリシーを作成する方法について説明します。

### 始める前に

リモート ロケーションのテクニカル サポート ポリシーを作成する場合は、まずリモート ロケーションを作成する必要があります。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[操作（Operations）]** を選択します。

**[インテント（Intent）]** の **[操作（Operations）]** オプションのリストが表示されます。

**ステップ 3** **[インテント（Intent）]** の **[操作（Operations）]** リストから、**[テクニカル サポートの作成（Create Tech Support）]** をクリックします。**[テクニカル サポートの作成（Create Tech Support）]** ダイアログ ボックスが表示されます。

**ステップ 4** 次の *[テクニカル サポートの作成ダイアログボックスのフィールド（Create Tech Support Dialog Box Fields）]* のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

表 *12 :* テクニカル サポートの作成ダイアログボックスのフィールド

| **[プロパティ（Properties）]** | **説明** |
|---|---|
| **全般** | |
| **名前** | テクニカル サポート ポリシーの名前を入力します。 |
| **説明** | テクニカル サポートの説明を入力します。 |
| **Settings** | |

| [プロパティ（Properties）] | 説明 |
|---|---|
| エクスポート先 | エクスポート先を選択します。<br>• コントローラ<br>• [リモート ロケーション（Remote Location）]：選択すると、[リモート ロケーションの選択（Select Remote Location）] オプションが表示されます。<br>1. [リモート ロケーションの選択（Select Remote Location）] をクリックします。[リモート ロケーションの選択（Select Remote Location）] ダイアログボックスが表示されます。<br>2. [[リモート ロケーションの選択（Select Remote Location）] ダイアログで、左側の列のリモート ロケーションをクリックして選択し、[選択（Select）] をクリックします。[テクニカル サポートの作成（Create Tech Support）] ダイアログボックスに戻ります。 |
| アップグレード前のログを含める | テクニカル サポート ポリシーにアップグレード前のログを含める場合は、[有効（Enabled）] チェックボックスをオンにします。 |
| 作成後のトリガー | ポリシーの作成後にテクニカル サポート ポリシーを作成する場合は、[有効] (デフォルト) チェックボックスをクリックしてオンにします。無効にするには、チェックボックスをオフにします。 |

**ステップ 5** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用したトリガー スケジューラの作成

このセクションでは、トリガー スケジューラの作成方法について説明します。

**ステップ 1** **インテント** アイコンをクリックします。[インテント（Intent）] メニューが表示されます。

**ステップ 2** [インテント（Intent）] 検索ボックスの下のドロップダウン□をクリックし、[操作（Operations）] を選択します。

[インテント（Intent）] の [操作（Operations）] オプションのリストが表示されます。

**ステップ 3** **[インテント（Intent）]** の **[操作（Operations）]** リストから、**[スケジューラの作成（Create Scheduler）]** をクリックします。**[トリガー スケジューラの作成（Create Trigger Scheduler）]** ダイアログボックスが表示されます。

**ステップ 4** 次の *[トリガー スケジューラの作成ダイアログボックスのフィールド（Create Scheduler Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

**表 *13*: トリガー スケジューラの作成ダイアログボックスのフィールド**

| **[プロパティ（Properties）]** | **説明** |
|---|---|
| **全般** | |
| **名前** | トリガー スケジューラ ポリシーの名前を入力します。 |
| **説明** | トリガーの説明を入力します。 |
| **Settings** | |

| [プロパティ（**Properties**）] | 説明 |
| --- | --- |
| 繰り返しウィンドウ | **[繰り返しウィンドウの追加（Add Recurring Window）]** をクリックします。**[繰り返しウィンドウの追加（Add Recurring Window）]** ダイアログウィンドウが表示されます。<br>1. **[スケジュール（Schedule）]** ドロップダウンリストから、次のいずれかを選択します。<br>• 毎日<br>• 月曜日<br>• 火曜日<br>• 水曜日<br>• 木曜日<br>• 金曜日<br>• 土曜日<br>• 日曜日<br>• 奇数日<br>• 偶数日<br>2. **[開始時間（Start Time）]** フィールドに、時間を入力します。<br>3. **[最大同時タスク数（Maximum Concurrent Tasks）]** フィールドから数値を入力するか、フィールドを空白のままにして無制限を指定します。<br>4. **[最大実行時間（Maximum Running Time）]** で、**[無制限（Unlimited）]** または **[カスタム（Custom）]** をクリックして選択します。<br>5. 終了したら、[Add] をクリックします。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| ワンタイム ウィンドウの追加 | **[ワンタイムウィンドウの追加（Add One Time Window）]** をクリックします。**[ワンタイムウィンドウの追加（Add One Time Window）]** ダイアログが表示されます。<br>1. **[開始時間（Start Time）]** フィールドに、時間を入力します。<br>2. **[最大同時タスク数（Maximum Concurrent Tasks）]** フィールドに数値を入力するか、フィールドを空白のままにして無制限を指定します。<br>3. **[最大実行時間（Maximum Running Time）]** で、**[無制限（Unlimited）]** または **[カスタム（Custom）]** をクリックして選択します。<br>4. 終了したら、[Add] をクリックします。 |

**ステップ 5** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用したリモート ロケーションの作成

このセクションでは、Cisco Cloud APIC を使用したリモート ロケーションの作成方法について説明します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[操作（Operations）]** を選択します。

**[インテント（Intent）]** の **[操作（Operations）]** オプションのリストが表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[操作（Operations）]** リストで、**[リモート ロケーションの作成（Create Remote Location）]** をクリックします。**[リモート ロケーションの作成（Create Remote Location）]** ダイアログボックスが表示されます。

**ステップ 4** 次の *[リモート ロケーションの作成ダイアログボックスのフィールド（Create Remote Location Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

**表 *14 :* リモート ロケーションの作成ダイアログボックスのフィールド**

| [プロパティ（Properties）] | 説明 |
|---|---|
| 全般 | |

| [プロパティ（Properties）] | 説明 |
|---|---|
| 名前 | リモート ロケーション ポリシーの名前を入力します。 |
| 説明 | リモート ロケーション ポリシーの説明を入力します。 |
| **Settings** | |
| **Hostname/IP Address** | リモート ロケーションのホスト名または IP アドレスを入力します |
| **Protocol** | プロトコルを選択します。<br>• **FTP**<br>• **SFTP**<br>• **SCP** |
| **Path** | リモート ロケーションのパスを入力します。 |
| **Port** | リモート ロケーションのポートを入力します。 |
| **Username** | リモートロケーションのユーザー名を入力します。 |
| 認証タイプ | SFTP または SCP を使用する場合は、認証タイプを選択します。<br>• **[Password]**<br>• **SSH キー（SSH Key）** |
| **SSH キー コンテンツ** | SSH キーのコンテンツを入力します。 |
| **SSH キー パスフレーズ** | SSH キー パスフレーズ |
| **Password** | リモート ロケーションにアクセスするためのパスワードを入力します。 |
| **Confirm Password** | リモート ロケーションにアクセスするためのパスワードを再入力します。 |
| 管理EPG | 1. **[管理EPGの選択]** をクリックします。**[管理EPGの選択]** ダイアログが表示されます。<br>2. 左側の列で、をクリックして管理EPGを選択します。<br>3. [選択（Select）] をクリックします。 |

**ステップ 5** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用したローカル ドメインの作成

このセクションでは、クラウドAPIC GUIを使用したログイン ドメインの作成方法について説明します。

### 始める前に

非ローカルドメインを作成する前に、プロバイダーを作成します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[ログイン ドメインの作成（Create Login Domain）]** をクリックします。**[ログイン ドメインの作成（Create Login Domains）]** ダイアログボックスが表示されます。

**ステップ 4** 次の *[ログイン ドメインダイアログボックスのフィールド（Login Domains Dialog Box Fields）]* のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

**表 *15:* ログイン ドメインダイアログボックスの作成のフィールド**

| **[プロパティ（Properties）]** | **説明** |
|---|---|
| **名前（Name）** | ログイン ドメインの名前を入力します。 |
| **説明** | ログイン ドメインの説明を入力します。 |
| **レルム** | レルムを選択します。<br>• **Local**<br>• **LDAP**：プロバイダーを追加し、認証タイプを選択する必要があります。<br>• **RADIUS**：プロバイダーを追加する必要があります。<br>• **TACACS+**：プロバイダーの追加が必要です。<br>• **SAML**：プロバイダーの追加が必要です。 |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| プロバイダ | プロバイダーを追加するには、次の手順を実行します。<br>1. **[プロバイダーの追加（Add Providers）]** をクリックします。**[プロバイダーの選択（Select Providers）]** ダイアログが表示され、左側のペインにプロバイダーのリストが表示されます。<br>2. クリックしてプロバイダーを選択します。<br>3. **[選択 (Select)]** をクリックして、プロバイダを追加します。 |
| 詳細設定 | **[認証タイプ（Authentication Type）]** および **[LDAP グループ マップ ルール（LDAP Group Map Rules）]** フィールドを表示します。 |
| 認証タイプ | レルム オプションにLDAP を選択した場合は、次のいずれかの認証タイプを選択します。<br>• **Cisco AV ペア**：（デフォルト）<br>• **LDAP グループ マップ ルール**：LDAP グループ マップ ルールを追加する必要があります。 |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| LDAP グループ マップ ルール | |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | LDAP グループ マップ ルールを追加するには、次の手順を実行します。<br>1. **[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** をクリックします。**[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** ダイアログが表示され、左側のペインにプロバイダーのリストが表示されます。<br>2. **[名前（Name）]** フィールドに、ルールの名前を入力します。<br>3. **[説明（Description）]** フィールドに、ルールの説明を入力します。<br>4. **[グループ DN（Group DN）]** フィールドにルールのグループ DN を入力します。<br>5. セキュリティ ドメインの追加：<br>1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログ ボックスが表示されます。<br>2. **[セキュリティ ドメインの選択（Select Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログボックスが表示され、左側のウィンドウにセキュリティ ドメインのリストが表示されます。<br>3. セキュリティ ドメインをクリックして選択します。<br>4. **[選択（Select）]** をクリックして、セキュリティ ドメインを追加します。**[セキュリティ ドメインの追加（Add Security Domain）] ダイアログボックスに戻ります。**<br>5. ユーザー ロールを追加する:<br>1. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスで、**[ロールの選択（Select Role）]** をクリックします。**[ロールの選択（Select Role）]** ダイアログボックスが表示され、左側のペインにロールのリストが表 |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | 示されます。<br>2. クリックしてロールを選択します。<br>3. **[選択（Select）]** をクリックしてロールを追加します。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスに戻ります。<br>4. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスから、**[権限タイプ（Privilege Type）]** ドロップダウンリストをクリックして、**[読み取り権限（Read Privilege）]** または **[書き込み権限（Write Privilege）]** を選択します。<br>5. **[権限タイプ（Privilege Type）]** ドロップダウン リストの右側のチェックマークをクリックして、確認します。<br>6. 終了したら、[Add] をクリックします。**[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** ダイアログボックスに戻り、別のセキュリティドメインを追加できます。 |

**ステップ 5** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用したプロバイダーの作成

このセクションでは、クラウド APIC GUI を使用したプロバイダーの作成方法について説明します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[プロバイダーの作成（Create Provider）]** をクリックします。**[プロバイダーの作成（Create Provider）]** ダイアログボックスが表示されます。

**ステップ 4** 次の *[プロバイダーの作成ダイアログボックスのフィールド（Create Provider Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

**表 *16* : プロバイダーの作成ダイアログボックスのフィールド**

| **[プロパティ（Properties）]** | **説明** |
|---|---|
| **ホスト名/IP アドレス** | プロバイダーのホスト名またはIPアドレスを入力します。 |
| **説明** | プロバイダーの説明を入力します。 |
| **タイプ（Type）** | **[タイプ（Type）]** ドロップダウン リストから、次のいずれかのタイプを選択します。<br>• **LDAP**<br>• **RADIUS**<br>• **TACACS+**<br>• **SAML**<br>（注） 選択したタイプに基づいて一連のフィールドが表示されます。 |
| **[LDAP] 設定** | |
| **[バインド DN（Bind DN）]** | LDAP バインド DN を入力します。 |
| **[ベース DN（Base DN）]** | LDAP ベース DN を入力します。 |
| **Password** | LDAP 設定のパスワードを入力します。 |
| **Confirm Password** | LDAP 設定のパスワードを再入力します。 |
| **[ポート（Port）]** | プロバイダー タイプのポート番号を入力します。 |
| **詳細設定** | プロバイダーダイアログボックスの **[設定]** セクションに追加フィールドを表示します。 |
| **タイムアウト(秒)** | タイムアウトが発生するまでの許容秒数を入力します。デフォルトは 30 です。 |
| **リトライ（Retries）** | 許可された再試行数を設定します。デフォルトは 1 です。 |
| **[SSL]** | SSL を有効にするには、**[SSL]** チェックボックスをクリックしてオンにします。SSLを無効にするには、**[SSL]** チェック ボックスをクリックしてオフにします。デフォルトではイネーブルになっています。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| SSL証明書の検証レベル | 次のいずれかを実行します。<br>• 許可<br>• 厳格な設定(RFC2821準拠) |
| [Attribute] | [属性] テキスト ボックスに LDAP 属性を入力します。 |
| フィルタタイプ | フィルタ タイプを選択します。<br>• Default<br>• Microsoft AD<br>• Custom |
| フィルタ（Filter） | テキストボックスにLDAPフィルタを入力します。このオプションは、カスタム フィルタ タイプが選択されている場合にのみ表示されます。 |
| [管理 EPG の選択（Select Management EPG）] | 管理 EPG を追加するには:<br>1. [管理 EPG の選択（Select Management EPG）] をクリックします。[ロールの選択（Select Role）] ダイアログボックスが表示され、左側のペインにロールのリストが表示されます。<br>2. クリックして EPG を選択します。<br>3. [選択] をクリックして、管理 EPG を LDAP に追加します。 |
| サーバーモニタリング | サーバーの監視を有効にするには、[有効] チェックボックスをクリックしてオンにします。サーバーの監視を無効にするには、[有効] チェック ボックスをクリックしてオフにします。デフォルトではディセーブルになっています。 |
| [RADIUS] 設定 | |
| Key | RADIUS キーを入力します。 |
| 確認キー | RADIUS キーを再入力します。 |
| 詳細設定 | プロバイダー ダイアログ ボックスの [設定] セクションに追加フィールドを表示します。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| [ポート（Port）] | RADIUS 設定のポート番号を入力します。デフォルトは 1812 です。 |
| [認証プロトコル（Authentication Protocol）] | 次の中から選択します。<br>• **PAP**：（デフォルト）<br>• **CHAP**<br>• **MS-CHAP** |
| タイムアウト(秒) | タイムアウトが発生するまでの許容秒数を入力します。デフォルトは 5 分です。 |
| リトライ（Retries） | 許可された再試行数を設定します。デフォルトは 1 です。 |
| [管理 EPG の選択（Select Management EPG）] | 管理 EPG を追加するには:<br>1. **[管理 EPG の選択（Select Management EPG）]** をクリックします。**[ロールの選択（Select Role）]**ダイアログボックスが表示され、左側のペインにロールのリストが表示されます。<br>2. クリックして EPG を選択します。<br>3. **[選択]** をクリックして、管理 EPG を RADIUS に追加します。 |
| サーバーモニタリング | サーバーの監視を有効にするには、**[有効]** チェックボックスをクリックしてオンにします。サーバーの監視を無効にするには、**[有効]** チェックボックスをクリックしてオフにします。デフォルトではディセーブルになっています。 |
| **[TACACS+] 設定** | |
| Key | TACACS+ キーを入力します。 |
| 確認キー | TACACS+ キーを再入力します。 |
| 詳細設定 | プロバイダーダイアログボックスの **[設定]** セクションに追加フィールドを表示します。 |
| [ポート（Port）] | TACACS+設定用のポート番号を入力します。デフォルトは 1812 です。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| [認証プロトコル（Authentication Protocol）] | 次の中から選択します。<br>• **CHAP**<br>• **MS-CHAP**<br>• **PAP**：（デフォルト） |
| タイムアウト(秒) | タイムアウトが発生するまでの許容秒数を入力します。デフォルトは 5 分です。 |
| リトライ（Retries） | 許可された再試行数を設定します。デフォルトは 1 です。 |
| [管理 EPG の選択（Select Management EPG）] | 管理 EPG を追加するには:<br>1. **[管理 EPG の選択（Select Management EPG）]** をクリックします。**[ロールの選択（Select Role）]** ダイアログボックスが表示され、左側のペインにロールのリストが表示されます。<br>2. クリックして EPG を選択します。<br>3. **[選択]** をクリックして、管理 EPG を TACACS+ に追加します。 |
| サーバーモニタリング | サーバーの監視を有効にするには、**[有効]** チェックボックスをクリックしてオンにします。サーバーの監視を無効にするには、**[有効]** チェック ボックスをクリックしてオフにします。デフォルトではディセーブルになっています。 |
| **[SAML] 設定** | |
| ID プロバイダー | 次のアイデンティティ プロバイダーから選択します。<br>• **ADFS**：（デフォルト）<br>• **OKTA**<br>• **PING アイデンティティ** |
| [IDプロバイダーのメタデータのURL（Identity Provider Metadata URL）] | アイデンティティ プロバイダーから提供されたメタデータ URL を入力します。 |
| Entity ID | SAML エンティティ識別子として一意の ID を入力します。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| メタデータ URL の HTTPS プロキシ | ID プロバイダーのメタデータ URL にアクセスするために使用される HTTPS プロキシを入力します。 |
| 詳細設定 | プロバイダーダイアログボックスの **[設定]** セクションに追加フィールドを表示します。 |
| GUI リダイレクト バナー メッセージ (URL) | GUI リダイレクトバナーメッセージを入力します。 |
| 認証局 | 認証局を選択するには：<br>1. **[認証局の選択（Select Certificate Authority）]** をクリックします。**[認証局の選択（Select Certificate Authority）]** ダイアログが表示され、左側のペインに証明書のリストが表示されます。<br>2. クリックして証明書を選択します。<br>3. **[選択]** をクリックして証明書を追加します。**[プロバイダーの作成（Create ）]** ダイアログボックスに戻ります。 |
| タイムアウト(秒) | タイムアウトが発生するまでの許容秒数を入力します。デフォルトは 5 分です。 |
| リトライ（Retries） | 許可された再試行数を設定します。デフォルトは 1 です。 |
| [署名アルゴリズム認証ユーザー要求（Signature Algorithm Authentication User Requests）] | **[リクエストの署名アルゴリズム]** ドロップダウンリストをクリックし、次のいずれかを選択します。<br>• **RSA SHA1**<br>• **RSA SHA224**<br>• **RSA SHA256**<br>（デフォルト）<br>• **RSA SHA384**<br>• **RSA SHA512** |
| SAML認証要求の署名 | 有効にするには、チェックボックスをクリックしてチェックを入れます。無効にするには、チェックボックスをクリックしてチェックを外します。デフォルトではイネーブルになっています。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| SAML応答メッセージの署名 | 有効にするには、チェックボックスをクリックしてチェックを入れます。無効にするには、チェックボックスをクリックしてチェックを外します。デフォルトではイネーブルになっています。 |
| SAML応答の署名アサーション | 有効にするには、チェックボックスをクリックしてチェックを入れます。無効にするには、チェックボックスをクリックしてチェックを外します。デフォルトではイネーブルになっています。 |
| SAMLアサーションの暗号化 | 有効にするには、チェックボックスをクリックしてチェックを入れます。無効にするには、チェックボックスをクリックしてチェックを外します。デフォルトではイネーブルになっています。 |

**ステップ 5** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用したセキュリティ ドメインの作成

セキュリティドメインは、追加するセキュリティドメインにテナントを制限します。セキュリティドメインを追加しない場合、すべてのセキュリティドメインがこのテナントにアクセスできます。このセクションでは、GUI を使用してセキュリティ ドメインを作成する方法について説明します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

**ステップ 3** [Intent]メニューの[Administrative]リストで、[Create Security Domain]をクリックします。**[セキュリティ ドメインの作成（Create Security Domain）]** ダイアログ ボックスが表示されます。

**ステップ 4** **[名前（Name）]** フィールドに、セキュリティ ドメインの名前を入力します。

**ステップ 5** **[説明（Description）]** フィールドに、セキュリティ ドメインの説明を入力します。

**ステップ 6** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用したロールの作成

このセクションでは、クラウド APIC GUI を使用したロールの作成方法について説明します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

**ステップ 3** **[Intent]** メニューの **[Administrative]** リストで、**[セキュリティ ドメインの作成（Create Security Domain）]** をクリックします。**[ロールの作成（Create Role）]** ダイアログ ボックスが表示されます。

**ステップ 4** 次の *[ロールの作成ダイアログボックスのフィールド（Create Role Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

**表 *17*: ロールの作成ダイアログボックスのフィールド**

| **[プロパティ（Properties）]** | **説明** |
|---|---|
| **全般** | |
| **名前** | **[Name]** フィールドにロール名を入力します。 |
| **説明** | ロールの説明を入力します。 |
| **Settings** | |

| [プロパティ（**Properties**）] | 説明 |
| --- | --- |
| 特権 | |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | クリックして、ユーザに割り当てる権限のチェックボックスをオンにします。権限は次のとおりです。<br>• **aaa**：認証、許可、アカウンティング、インポート/エクスポート ポリシーの設定に使用されます。<br>• **access-connectivity-l1** インフラの下のレイヤ 1 設定に使用されます。例：セレクタとポート レイヤ 1 のポリシー設定。<br>• **access-connectivity-l2** ：インフラの下のレイヤ 2 設定に使用されます。例：セレクタおよび接続可能なエンティティ設定をカプセル化します。<br>• **access-connectivity**：インフラでのレイヤ 3 の設定、テナントの L3Out でのスタティック ルート設定に使用されます。<br>• **access-connectivity-mgmt** ：管理インフラ ポリシーに使用されます。<br>• **access-connectivity-util** ：テナント ERSPAN ポリシーに使用されます。<br>• **access-equipment**：アクセスポートの設定に使用されます。<br>• **access-protocol-l1** ：インフラのレイヤ 1 プロトコル設定に使用されます。<br>• **access-protocol-l2** ：インフラのレイヤ 2 プロトコル設定に使用されます。<br>• **access-protocol-l3** ：インフラでのレイヤ 3 プロトコル設定に使用されます。<br>• **access-protocol-mgmt** ：NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシーに使用されます。<br>• **access-protocol-ops** ：クラスタ ポリシーやファームウェア ポリシーなどの操作関連のアクセス ポリシーに使用されます。<br>• **access-protocol-util** ：テナント ERSPAN ポリシーに使用されます。<br>• **access-qos**：CoPP および QoS に関連するポリシーの変更に使用されます。 |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | • **admin**：すべてへのアクセス（すべてのロールの組み合わせ）<br>• **fabric-connectivity-l1** ：ファブリックの下のレイヤ 1 設定に使用されます。例：セレクタおよびポート レイヤ 1 のポリシーと vPC 保護。<br>• **fabric-connectivity-l2** ：ポリシー展開の影響を推定するための警告を生成するために、ファームウェアおよび展開ポリシーで使用されます。<br>• **fabric-connectivity-l3** ：ファブリックの下のレイヤ 3 設定に使用されます。例: ファブリック IPv4 および MAC 保護グループ。<br>• **fabric-connectivity-mgmt**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、および診断ポリシーに使用されます。<br>• **fabric-connectivity-util**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。<br>• **fabric-equipment**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。<br>• **fabric-protocol-l1** ：ファブリックの下のレイヤ 1 プロトコル設定に使用されます。<br>• **fabric-protocol-l2** ：ファブリックの下のレイヤ 2 プロトコル設定に使用されます。<br>• **fabric-protocol-l3** ：ファブリックの下のレイヤ 3 プロトコル設定に使用されます。<br>• **fabric-protocol-mgmt** ：NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシーに使用されます。<br>• **fabric-protocol-ops** ：ERSPAN およびヘルス スコア ポリシーに使用されます。<br>• **fabric-protocol-util** ：ファームウェア管理の traceroute およびエンドポイント トラッキング ポリシーに使用されます。<br>• **none**：特権なし。 |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | • **nw-svc-device** ：レイヤ 4 からレイヤ 7 のサービス デバイスを管理するために使用されます。<br>• **nw-svc-devshare** ：共有レイヤ 4 ～ レイヤ 7 サービス デバイスの管理に使用されます。<br>• **nw-svc-params**：レイヤ 4 ～ レイヤ 7 のサービス ポリシーの管理に使用されます。<br>• **nw-svc-policy**：レイヤ 4 ～ レイヤ 7 のネットワーク サービス オーケストレーションの管理に使用されます。<br>• **ops**：アトミック カウンタ、SPAN、TSW、技術サポート、トレースルート、分析、コア ポリシーなど、ポリシーのモニタリングとトラブルシューティングを含む動作ポリシーに使用されます。<br>• **tenant-connectivity-l1** ：ブリッジ ドメインやサブネットなど、レイヤ 1 接続の変更に使用されます。<br>• **tenant-connectivity-l2** ：ブリッジ ドメインやサブネットなど、レイヤ 2 接続の変更に使用されます。<br>• **tenant-connectivity-l3** ：VRF を含むレイヤ 3 接続の変更に使用されます。<br>• **tenant-connectivity-mgmt** ：テナントのインバンドおよびアウトオブバンドの管理接続構成、およびアトミック カウンターやヘルス スコアなどのポリシーのデバッグ/監視に使用されます。<br>• **tenant-connectivity-util**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。<br>• **tenant-epg**：エンドポイント グループ、VRF、ブリッジ ドメインの削除/作成など、テナント設定の管理に使用されます。<br>• **tenant-ext-connectivity-l2**：テナントの L2Out 構成を管理するために使用されます。<br>• **tenant-ext-connectivity-l3**：テナント L3Out 構成の管理に使用されます。 |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | • **tenant-ext-connectivity-mgmt**：ファームウェア ポリシーの書き込みアクセスとして使用されます。<br>• **tenant-ext-connectivity-util** ： traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。<br>• **tenant-ext-protocol-l1**：テナントの外部レイヤ 1 プロトコルの管理に使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。<br>• **tenant-ext-protocol-l2** ：テナントの外部レイヤ 2 プロトコルの管理に使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。<br>• **tenant-ext-protocol-l3** ：BGP、OSPF、PIM、IGMP などのテナントの外部レイヤ 3 プロトコルを管理するために使用されます。<br>• **tenant-ext-protocol-mgmt**：ファームウェア ポリシーの書き込みアクセスとして使用されます。<br>• **tenant-ext-protocol-util**：traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。<br>• **tenant-network-profile**：ネットワーク プロファイルの削除および作成、エンドポイント グループの削除および作成など、テナント設定の管理に使用されます。<br>• **tenant-protocol-l1** ：テナントの下でレイヤ 1 プロトコルの設定を管理するために使用されます。<br>• **tenant-protocol-l2** ：テナントの下でレイヤ 2 プロトコルの設定を管理するために使用されます。<br>• **tenant-protocol-l3** ：テナントの下でレイヤ 3 プロトコルの設定を管理するために使用されます。<br>• **tenant-protocol-mgmt**：ファームウェア ポリシーの書き込みアクセスとして使用されます。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| | • **tenant-protocol-ops** ：テナント traceroute ポリシーに使用されます。<br>• **tenant-protocol-util** — traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。<br>• **tenant-qos**：ファームウェア ポリシーの書き込みアクセスとしてのみ使用されます。<br>• **tenant-security**：テナントの契約関連の設定に使用されます。<br>• **vmm-connectivity**：VM 接続に必要な APIC の VMM インベントリ内のすべてのオブジェクトを読み取るために使用されます。<br>• **vmm-ep**：APIC の VMM インベントリ内の VM およびハイパーバイザーエンドポイントを読み取るために使用されます。<br>• **vmm-policy**：VM ネットワーキングのポリシーの管理に使用されます。<br>• **vmm-protocol-ops**：VMM ポリシーでは使用されません。<br>• **vmm-security**：テナントの契約関連の設定に使用されます。 |

**ステップ 5** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用した RBAC ルールの作成

このセクションでは、GUI を使用して RBAC ルールを作成する方法について説明します。

**始める前に**

セキュリティ ドメインの作成

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

**[インテント（Intent）]** メニューに**管理**オプションのリストが表示されます。

**ステップ 3** **[Intent]** メニューの **[Administrative]** リストで、**[RBAC ルールの作成（Create RBAC Rule）]** をクリックします。**[RBAC ルールの作成（Create RBAC Rule）]** ダイアログボックスが表示されます。

**ステップ 4** **DN** フィールドに、ルールの DN を入力します。

**ステップ 5** セキュリティ ドメインを選択します。

a) **[セキュリティ ドメインの選択（Select Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログ ボックスが表示されます。

b) **[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログで、左側の列のセキュリティ ドメインをクリックして選択し、**[選択（Select）]** をクリックします。**[RBAC ルールの作成]** ダイアログ ボックスに戻ります。

**ステップ 6** **[書き込みを許可]** フィールドで、**[はい]** をクリックして書き込みを許可するか、**[いいえ]** をクリックして書き込みを許可しません。

**ステップ 7** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用した認証局の作成

ここでは、GUI を使用して認証局を作成する方法について説明します。

### 始める前に

- 証明書チェーン（certificate chain）を設定します。
- 認証局がテナント用の場合は、テナントを作成します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

**[インテント（Intent）]** メニューに**管理**オプションのリストが表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[証明書認証局の作成（Create Certificate Authority）]** をクリックします。**[証明書認証局の作成（Create Certificate Authority）]** ダイアログボックスが表示されます。

**ステップ 4** *[*証明書認証局の作成ダイアログボックスのフィールド（*Create Certificate Authority Dialog Box Fields*）*]* のテーブルにリストされた各フィールドに適切な値を入力して、続行します。

**表 *18 :* 証明書認証局の作成ダイアログボックスのフィールド**

| **[プロパティ（Properties）]** | **説明** |
|---|---|
| **名前（Name）** | 証明書認証局の名前を入力してください。 |
| **説明** | 証明書認証局の説明を入力してください。 |

| [プロパティ（Properties）] | 説明 |
|---|---|
| 用途 | 次のオプションから選択します。<br>• テナント（Tenant）：認証局が特定のテナント用かどうかを選択します。選択すると、[テナントの選択（Select Tenant）] オプションがGUIに表示されます。<br>• システム（System）：認証局がシステム用である場合に選択します。 |
| テナントの選択 | テナントを選択します。<br>1. [テナントの選択（Select Tenant）] をクリックします。[テナントの選択（Select Tenant）] ダイアログボックスが表示されます。<br>2. [テナントの選択（Select Tenant）] ダイアログで、左側の列のテナントをクリックして選択し、[選択（Select）] をクリックします。[証明書認証局の作成（Create Certificate Authority）] ダイアログボックスが表示されます。 |
| Certificate Chain | [証明書チェーン (Certificate Chain)] フィールドに、証明書チェーンを入力します。<br>（注） チェーンの証明書を次の順序で追加します。<br>1. CA<br>2. Sub-CA<br>3. サブサブCA<br>4. サーバー |

**ステップ 5** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用したキー リングの作成

このセクションでは、Cisco Cloud APIC GUI を使用したキー リングの作成方法について説明します。

始める前に

- 認証局を作成します。
- 証明書を持っています。
- キー リングが特定のテナント用である場合は、テナントを作成します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[キー リングの作成（Create Key Ring）]** をクリックします。**[キー リングの作成（Create Key Ring）]** ダイアログ ボックスが表示されます。

**ステップ 4** 次の *[*キー リングの作成ダイアログボックスのフィールド（*Create Key Ring Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *19 :* キー リングの作成ダイアログボックスのフィールド

| **[プロパティ（Properties）]** | 説明 |
|---|---|
| 名前（**Name**） | キー リングの名前を入力します。 |
| 説明 | キー リングの説明を入力します。 |
| 用途 | • **System**：キー リングはシステム用です。<br>• **Tenant**：キー リングは特定のテナント用です。テナントを指定する **[テナント（Tenant）]** フィールドを表示します。 |
| テナントの選択 | テナントを選択します。<br>1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。<br>2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[キー リングの作成（Create Key Ring）]** ダイアログボックスに戻ります。 |
| **Settings** | |

| [プロパティ（Properties）] | 説明 |
|---|---|
| 認証局 | 認証局を選択するには：<br>1. **[認証局の選択（Select Certificate Authority）]** をクリックします。**[認証局の選択（Select Certificate Authority）]** ダイアログが表示されます。<br>2. 左側の列で認証局をクリックして選択します。<br>3. **[選択（Select）]** をクリックします。**[キー リングの作成（Create Key Ring）]** ダイアログボックスに戻ります。 |
| 秘密キー（Private Key） | 次のいずれかを選択します。<br>• **[新しいキーの生成（Generate New Key）]**：新しいキーを生成します。<br>• **[既存のキーのインポート（Import Existing Key）]**：**[秘密キー（Private Key）]** テキスト ボックスが表示され、既存のキーを使用できます。 |
| 秘密キー（Private Key） | **[秘密キー（Private Key）]** テキスト ボックスに既存のキーを入力します（**[既存のキーのインポート（Import Existing Key）]** オプションの場合）。 |
| Modulus | **[モジュール（Modulus）]** ドロップダウン リストをクリックし、次の項目の中から選択します。<br>• **MOD 512**<br>• **MOD 1024**<br>• **MOD 1536**<br>• **MOD 2048**：デフォルト |
| 証明書 | **[証明書（Certificate）]** テキスト ボックスに証明書情報を入力します。 |

**ステップ 5** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用したローカル ユーザーの作成

このセクションでは、クラウド APIC GUI を使用したローカル ユーザーの作成方法について説明します。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

**ステップ 3** **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[ローカル ユーザーの作成（Create Local User）]** をクリックします。**[ローカル ユーザーの作成（Create New User）]** ダイアログボックスが表示されます。

**ステップ 4** 次の *[ローカル ユーザーの作成ダイアログボックスのフィールド（Create Local User Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

**表 *20 :* ローカル ユーザーの作成ダイアログボックスのフィールド**

| **[プロパティ（Properties）]** | **説明** |
|---|---|
| **名前（Name）** | ローカル ユーザーのユーザー名を入力します。 |
| **Password** | ローカル ユーザーのパスワードを入力します。 |
| **Confirm Password** | ローカル ユーザーのパスワードを再入力します。 |
| **説明** | ローカル ユーザーの説明を入力します。 |
| **Settings** | |
| **アカウント ステータス** | アカウント ステータスを選択するには、次の手順を実行します。<br>• **Active**：ローカル ユーザー アカウントをアクティブにします。<br>• **Inactive**：ローカル ユーザー アカウントを非アクティブにします。 |
| **[名（First Name）]** | ローカル ユーザーの名を入力します。 |
| **姓（Last Name）** | ローカル ユーザーの姓を入力します。 |
| **電子メール アドレス（Email Address）** | ローカル ユーザーの E メール アドレスを入力します。 |
| **Phone Number** | ローカル ユーザーの 電話番号を入力します。 |

| [プロパティ（**Properties**）] | 説明 |
| --- | --- |
| セキュリティ ドメイン | |

| [プロパティ（Properties）] | 説明 |
| --- | --- |
| | セキュリティ ドメインを追加するには、次の手順を実行します。<br>1. **[セキュリティ ドメインの追加（Add Security Domain）]**をクリックします。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログ ボックスが表示されます。<br>2. **[セキュリティ ドメインの選択（Select Security Domain）]**をクリックします。**[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログボックスが表示され、左側のウィンドウにセキュリティ ドメインのリストが表示されます。<br>3. セキュリティ ドメインをクリックして選択します。<br>4. **[選択（Select）]**をクリックして、セキュリティ ドメインを追加します。**[セキュリティ ドメインの追加（Add Security Domain）] ダイアログボックスに戻ります。**<br>5. ユーザー ロールを追加する:<br>1. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスで、**[ロールの選択（Select Role）]** をクリックします。**[ロールの選択（Select Role）]** ダイアログ ボックスが表示され、左側のペインにロールのリストが表示されます。<br>2. クリックしてロールを選択します。<br>3. **[選択（Select）]** をクリックしてロールを追加します。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスに戻ります。<br>4. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログ ボックスから、**[権限タイプ（Privilege Type）]** ドロップダウン リストをクリックして、**[読み取り権限（Read Privilege）]** または **[書き込み権限（Write Privilege）]** を選択します。<br>5. **[権限タイプ（Privilege Type）]** ドロップダウンリストの右側のチェックマークをクリッ |

| [プロパティ（Properties）] | 説明 |
|---|---|
| | クして、確認します。<br>6. 終了したら、[Add]をクリックします。**[ローカル ユーザーの作成（Create Local User）]** ダイアログボックスに戻り、別のセキュリティ ドメインを追加できます。 |

**ステップ 5** **[高度な設定（Advanced Settings）]**をクリックして、*[*ローカルユーザーの作成ダイアログボックスのフィールド：高度な設定（*Create Local User Dailog Box Fields: Advanced Settings*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

**表 *21 :* ローカル ユーザーの作成ダイアログボックスのフィールド：高度な設定**

| プロパティ | 説明 |
|---|---|
| **Account Expires** | **[はい（Yes）]**を選択すると、アカウントは選択した時点で期限切れになるように設定されます。 |
| パスワードの更新が必要です | **[はい（Yes）]**を選択した場合、ユーザーは次回ログイン時にパスワードを変更する必要があります。 |
| **OTP** | ユーザーのワンタイムパスワード機能を有効にするには、チェックボックスをオンにします。 |
| ユーザー証明書 | ユーザー証明書を追加するには、次の手順を実行します。<br>1. **[X509 証明書の追加（Add X509 Certificate）]**をクリックします。**[X509 証明書の追加（Add X509 Certificate）]** ダイアログボックスが表示されます。<br>2. [Name] フィールドに名前を入力します。<br>3. **[ユーザー X509 証明書（User X509 Certificate）]** テキストボックスにX509証明書を入力します。<br>4. [Add] をクリックします。**[ユーザー X509 証明書の X509 証明書]** ダイアログボックスが閉じます。**[ローカル ユーザー]** ダイアログボックスに戻ります。 |

| プロパティ | 説明 |
| --- | --- |
| **SSH キー** | SSH キーを追加するには、次の手順を実行します。<br>1. **[SSH キーを追加（Add SSG Key）]** をクリックします。**[SSH キーの追加（Add SSG Key）]** ダイアログボックスが表示されます。<br>2. [Name] フィールドに名前を入力します。<br>3. **[キー（Key）]** テキストボックスに SSH キーを入力します。<br>4. [Add] をクリックします。**[SSH キーの追加（Add SSG Key）]** ダイアログボックスが閉じます。**[ローカル ユーザー]** ダイアログボックスに戻ります。 |

**ステップ 6** 設定が終わったら [Save] をクリックします。

# Cisco Cloud APIC GUI を使用したリージョンの管理（クラウド テンプレートの設定）

リージョンは、初回セットアップ時に構成されます。構成時に、Cisco Cloud APIC によって管理されるリージョンと、そのリージョンのサイト間およびリージョン間の接続を指定します。このセクションでは、初期インストール後に Cisco Cloud APIC GUI を使用してクラウド テンプレートでリージョンを管理する方法について説明します。

クラウドテンプレートの詳細については、クラウドテンプレートの概要を参照してください。

**ステップ 1** **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

**ステップ 2** **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[構成（Configuration）]** を選択します。

オプションのリストが **[インテント（Intent）]** メニューに表示されます。

**ステップ 3** **[インテント（Intent）]**メニューの **[構成（Configuration）]** リストで、**[クラウド APIC セットアップ（Cloud APIC Setup）]** をクリックします。
**[セットアップ - 概要]** ダイアログ ボックスが表示されます。

**ステップ 4** **[リージョン管理（Region Management）]** エリアで、**[設定の編集（Edit Configuration）]** をクリックします。
**[セットアップ - リージョン管理]** ダイアログ ボックスが表示されます。**セットアップ - リージョン管理**の一連のステップの最初のステップ、**管理するリージョン**が表示され、管理対象リージョンのリストが表示されます。

**ステップ 5** サイト間接続が必要な場合は、[サイト間接続（Inter-Site Connectivity）] 領域の [有効（Enabled）] ボックスをクリックしてオンにします。
このオプションを選択すると、ページ上部の**[セットアップ-リージョン管理（Setup-Region Management）]** の手順に**サイト間接続**の手順が追加されます。

**ステップ 6** Cisco Cloud APIC で管理するリージョンを選択するには、そのリージョンのチェック ボックスをクリックしてチェック マークを付けます。

**ステップ 7** クラウド ルータをこのリージョンにローカルに展開するには、そのリージョンの [Cloud Routers] チェック ボックスをオンにします。

**ステップ 8** クラウド サイトのファブリック インフラ接続を構成するには、**[次へ]** をクリックします。
**セットアップ- リージョン管理**の一連のステップの次のステップである、**一般的な接続**が表示されます。

**ステップ 9** CCR のサブネット プールを追加するには、**[クラウド ルータのサブネット プールを追加する（Add Subnet Pool for Cloud Router）]** をクリックし、テキスト ボックスにサブネットを入力します。

（注） クラウド APIC の導入時に提供される /24 サブネットは、最大 2 つのクラウド サイトに十分です。3 つ以上のクラウド サイトを管理する必要がある場合は、さらにサブネットを追加する必要があります。

**ステップ 10** **[CCR向け BGP 自律システム番号（BGP Autonomous System Number for CCRs）]** フィールドに値を入力します。

BGP ASN の範囲は 1 ー 65534 です。

**ステップ 11** **[Assign Public IP to CCR Interface（パブリック IP を CCR インターフェイスに割り当てる）]** フィールドで、CCR インターフェイスにパブリック IP アドレスまたはプライベート IP アドレスを割り当てるかどうかを決定します。

- パブリック IP アドレスを CCR インターフェイスに割り当てるには、**[有効（Enabled）]** チェック ボックスをオンのままにします。デフォルトでは、この **[有効]** チェック ボックスはオンになっています。
- パブリック IP アドレスを CCR インターフェイスに割り当てるには、**[有効（Enabled）]** チェック ボックスをオンのままにします。この場合、接続にはプライベート IP アドレスが使用されます。

（注） パブリック IP アドレスの無効化または有効化は中断を伴う操作であり、トラフィック損失の原因となる可能性があります。

リリース 5.2(1) 以降では、CCR に割り当てられたパブリック IP アドレスとプライベート IP アドレスの両方が、[クラウド リソース（Cloud Resources）] エリアにルータの他の詳細とともに表示されます。パブリック IP が CSR に割り当てられていない場合は、プライベート IP だけが表示されます。

**ステップ 12** リージョンごとのルーター数を選択するには、**[リージョンごとのルーター数]** ドロップダウン リストをクリックし、**[2]**、**[3]**、または **[4]** をクリックします。

**ステップ 13** **[ユーザー名（Username）]** テキストボックスにユーザー名を入力します。

**ステップ 14** **[パスワード（Password）]** テキスト ボックスと **[パスワードの確認（Confirm Password）]** テキスト ボックスに新しいパスワードを入力します。

**ステップ 15** スループット値を選択するには、**[ルーターのスループット]** ドロップダウン リストをクリックします。

（注）
- クラウド ルータは、ルータのスループットまたはログイン情報を変更する前に、すべてのリージョンから展開解除する必要があります。
- リリース 25.0(3) 以降、Cisco Cloud APIC は、Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V に移行します。Cisco Catalyst 8000V のスループット値については、Cisco Catalyst 8000V について を参照してください。

**ステップ 16** (オプション) ライセンス トークンを指定するには、**[ライセンス トークン]** テキスト ボックスに製品インスタンスの登録トークンを入力します。

（注）
- リリース 25.0(3) 以降、Cisco Cloud APIC は、Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V に移行します。Cisco Catalyst 8000V のライセンス情報については、Cisco Catalyst 8000V について を参照してください。
- トークンが入力されていない場合、CCR は EVAL モードになります。
- プライベート IP アドレスを使用して CCR のスマート ライセンスを登録する場合、パブリック IP アドレスが ステップ 11 （89 ページ） の CCR に対して無効になっている場合、サポートされる唯一のオプションは、**AWS Direct Connect または Azure Express Route to Cisco Smart Software Manager（CSSM）** です（**[管理用（Administrative）]** > **[スマート ライセンス（Smart Licensing）]** に移動して使用可能です）。この場合、AWS Direct Connect または Azure Express Route を介して CSSM への到達可能性を提供する必要があります。パブリック IP アドレスが無効になっている場合、プライベート IP アドレスが使用されているため、パブリック インターネットは使用できません。したがって、接続には AWS Direct Connect または Azure Express Route であるプライベート接続を使用する必要があります。

**ステップ 17** [次へ（Next）] をクリックします。
- これらの手順の前半で **[サイト間接続]** 領域の **[有効]** ボックスにチェック マークを付けた場合、**サイト間接続**は、**セットアップ - リージョン管理**の一連のステップの次のステップとして表示されます。ステップ 18 （90 ページ） に進みます。
- これらの手順の前半で **[サイト間接続]** 領域の **[有効]** ボックスにチェック マークを付けなかった場合は、ステップ 22 （90 ページ） に進みます。

**ステップ 18** テキスト ボックスにオンプレミスの IPsec トンネル ピアのピア パブリック IP アドレスを入力するには、**[IPSec トンネル ピアのパブリック IP を追加]** をクリックします。

**ステップ 19** **[エリア ID]** フィールドに OSPF エリア ID を入力します。

**ステップ 20** 外部サブネット プールを追加するには、**[外部サブネットの追加]** をクリックし、テキスト ボックスにサブネット プールを入力します。

**ステップ 21** すべての接続オプションを設定したら、ページの下部にある[次へ（Next）]をクリックします。

**ステップ 22** 終了したら **[Save and Continue（保存して続行）]** ボタンをクリックします。

# REST API を使用した Cisco Cloud APIC の構成

## REST API を使用したテナントの作成

このセクションでは、REST API を使用してテナントを作成する方法を示します。

テナントを作成するには:

```
<polUni>
  <fvTenant name="infra">
    <cloudAwsProvider region="us-east-1" accessKeyId="123" secretAccessKey="ABCDE" providerId="admin"
 status=""/>
  </fvTenant>
</polUni>
```

## REST API を使用したコントラクトの作成

この例では、REST API を使用して Cisco Cloud APIC のコントラクトを作成する方法を示します。

### 始める前に

フィルタを作成します。

コントラクトを作成するには：

**例**：

```
<polUni>
  <fvTenant name="t2" status="">
    <vzFilter descr="" name="http-family-destination" ownerKey="" ownerTag="">
      <vzEntry name="http" prot="tcp" etherT="ip" dFromPort="http" dToPort="http"/>
      <vzEntry name="https" prot="tcp" etherT="ip" dFromPort="https" dToPort="https"/>
    </vzFilter>
    <vzBrCP name="httpFamily">
      <vzSubj name="default" revFltPorts="yes" targetDscp="unspecified">
        <vzRsSubjFiltAtt action="permit" directives="" tnVzFilterName="http-family-destination"/>
      </vzSubj>
    </vzBrCP>
  </fvTenant>
</polUni>
```

# REST API を使用したクラウド コンテキスト プロファイルの作成

このセクションでは、クラウド コンテキスト プロファイルを作成する方法を示します。

### 始める前に

VRF を作成します。

**ステップ 1** リリース 25.0(2) より前のリリースの場合は、次のような投稿を入力して、クラウドコンテキストプロファイルを作成します。

例：

```
<polUni>
<fvTenant name="Corp1" status="">
 <cloudAwsProvider accessKeyId="" secretAccessKey="" providerId="aws" status="" accountId=""/>

   <fvCtx name="prod-1" status="">
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:400:400" type="export"/>
      <bgpRtTarget rt="route-target:as4-nn2:400:400" type="import"/>
    </bgpRtTargetP>
  </fvCtx>

   <fvCtx name="prod-2" status="">
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:500:500" type="export"/>
      <bgpRtTarget rt="route-target:as4-nn2:500:500" type="import"/>
    </bgpRtTargetP>
  </fvCtx>

  <cloudVpnGwPol name="VgwPol" status=""/>

  <cloudApp name="payment" status="">
    <cloudEPg  name="web" status="">
      <cloudRsCloudEPgCtx tnFvCtxName="prod-1" />
    </cloudEPg>
  </cloudApp>
  <cloudApp name="billing">
    <cloudEPg  name="app">
      <cloudRsCloudEPgCtx tnFvCtxName="prod-2" />
    </cloudEPg>
  </cloudApp>

  <cloudCtxProfile name="prod-web-east-1">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-east-1"/>
    <cloudRsToCtx tnFvCtxName="prod-1"/>
    <cloudRouterP name="RouterP1" type="vpn-gw">
     <cloudRsToVpnGwPol tnCloudVpnGwPolName="VgwPol"/>
       <cloudIntNetworkP name="IntNetworkP1"/>
    </cloudRouterP>

    <cloudCidr addr="60.10.10.1/16" primary="true">
        <cloudSubnet ip="60.10.10.1/24">
            <cloudRsZoneAttach tDn="uni/clouddomp/provp-aws/region-us-east-1/zone-us-east-1a"/>
        </cloudSubnet>
    </cloudCidr>
  </cloudCtxProfile>

  <cloudCtxProfile name="prod-payment-east-1" status="">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-east-1"/>
```

```
    <cloudRsToCtx tnFvCtxName="prod-2" status=""/>
    <cloudRouterP name="RouterP1" type="vpn-gw">
     <cloudRsToVpnGwPol tnCloudVpnGwPolName="VgwPol"/>
       <cloudIntNetworkP name="IntNetworkP1" status=""/>
    </cloudRouterP>

    <cloudCidr addr="70.10.10.1/16" primary="true" status="">
       <cloudSubnet ip="70.10.10.1/24" status="">
           <cloudRsZoneAttach tDn="uni/clouddomp/provp-aws/region-us-east-1/zone-us-east-1a"/>
       </cloudSubnet>
    </cloudCidr>
  </cloudCtxProfile>

</fvTenant>
</polUni>
```

**ステップ 2** リリース 25.0(2) 以降サポートされている **クラウド** アベイラビリティ ゾーンを使用してクラウド コンテキスト プロファイルを作成するには、次の例のような投稿を入力します。

リリース 25.0(2) 以降、**ユーザー** テナントでクラウド コンテキスト プロファイルを作成している場合、**クラウド** アベイラビリティ ゾーンのみに制限されます。クラウド アベイラビリティ ゾーンは、以下で強調表示されているゾーン フィールドを介して作成されます。クラウド アベイラビリティ ゾーンの詳細については、可用性ゾーン を参照してください。

**例**：

```
<polUni>
<fvTenant name="Corp1" status="">
 <cloudAwsProvider accessKeyId="" secretAccessKey="" providerId="aws" status="" accountId=""/>

   <fvCtx name="prod-1" status="">
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:400:400" type="export"/>
      <bgpRtTarget rt="route-target:as4-nn2:400:400" type="import"/>
    </bgpRtTargetP>
  </fvCtx>

   <fvCtx name="prod-2" status="">
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:500:500" type="export"/>
      <bgpRtTarget rt="route-target:as4-nn2:500:500" type="import"/>
    </bgpRtTargetP>
  </fvCtx>

  <cloudVpnGwPol name="VgwPol" status=""/>

  <cloudApp name="payment" status="">
    <cloudEPg  name="web" status="">
      <cloudRsCloudEPgCtx tnFvCtxName="prod-1" />
    </cloudEPg>
  </cloudApp>
  <cloudApp name="billing">
    <cloudEPg  name="app">
      <cloudRsCloudEPgCtx tnFvCtxName="prod-2" />
    </cloudEPg>
  </cloudApp>

  <cloudCtxProfile name="prod-web-east-1">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-east-1"/>
    <cloudRsToCtx tnFvCtxName="prod-1"/>
    <cloudRouterP name="RouterP1" type="vpn-gw">
     <cloudRsToVpnGwPol tnCloudVpnGwPolName="VgwPol"/>
       <cloudIntNetworkP name="IntNetworkP1"/>
```

```
    </cloudRouterP>
    <cloudCidr addr="10.10.0.0/16" primary="yes">
        <cloudSubnet ip="10.10.1.0/24" usage="gateway" scope="public" zone="”us-west-1a"/>
        <cloudSubnet ip="10.10.2.0/24" scope="public" zone="”us-west-1b"/>
    </cloudCidr>
  </cloudCtxProfile>

  <cloudCtxProfile name="prod-payment-east-1" status="">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-east-1"/>
    <cloudRsToCtx tnFvCtxName="prod-2" status=""/>
    <cloudRouterP name="RouterP1" type="vpn-gw">
     <cloudRsToVpnGwPol tnCloudVpnGwPolName="VgwPol"/>
       <cloudIntNetworkP name="IntNetworkP1" status=""/>
    </cloudRouterP>
    <cloudCidr addr="20.10.0.0/16" primary="yes">
        <cloudSubnet ip="20.10.1.0/24" scope="public" zone="”us-west-1a"/>
    </cloudCidr>
  </cloudCtxProfile>

</fvTenant>
</polUni>
```

# REST API を使用したクラウド リージョンの管理

このセクションでは、REST API を使用してクラウド リージョンを管理する方法を示します。

クラウド リージョンを作成するには:

```
<polUni>
  <cloudDomP name="dom-us-east-2">
    <cloudBgpAsP asn="64513"/>
    <cloudProvP vendor="aws">
      <cloudRegion name="us-east-2" adminSt="managed">
        <cloudZone name="us-east-2a"/>
        <cloudZone name="us-east-2b"/>
      </cloudRegion>
    </cloudProvP>
  </cloudDomP>
</polUni>
```

# REST API を使用したフィルタの作成

このセクションでは、REST API を使用してフィルタを作成する方法を示します。

フィルタを作成するには、次の手順を実行します。

```
https://<IP_Address>/api/node/mo/.xml
<polUni>
<fvTenant name="intervpc" >
<fvCtx name="VRF1"/>
```

```
    <cloudApp name="CloudAP1" >
    <cloudEPg name="CloudEPG1" >
        <cloudRsCloudEPgCtx tnFvCtxName="VRF1"/>
        <fvRsProv tnVzBrCPName="Contract2” > </fvRsProv>
        <cloudEPSelector name="sel1" matchExpression="custom:epgtag=='cloudepg1'" />
      </cloudEPg>
     </cloudApp>

      <vzFilter name="http" annotation="orchestrator:msc" >
      <vzEntry name="Entry3" prot="tcp" etherT="ipv4" arpOpc="unspecified" stateful="no"
applyToFrag="no" sFromPort="unspecified" sToPort="unspecified" dFromPort="80" dToPort="80" > </vzEntry>

    </vzFilter>

   <vzBrCP name="Contract2" scope="global">
      <vzSubj name="test-subj" >


        <vzRsSubjFiltAtt action="permit" tnVzFilterName="http" directives="none" />


      </vzSubj>
    </vzBrCP>
   </fvTenant>
</polUni>
```

# REST API を使用したアプリケーション プロファイルの作成

このセクションでは、REST API を使用してアプリケーション プロファイルを作成する方法を示します。

### 始める前に

テナントを作成します。

アプリケーション プロファイルを作成する方法：

```
https://<IP_Address>/api/node/mo/.xml
<polUni>
<fvTenant name="intervpc" >
<fvCtx name="VRF1"/>
    <cloudApp name="CloudAP1" >

    <cloudEPg name="CloudEPG1" >
        <cloudRsCloudEPgCtx tnFvCtxName="VRF1"/>
        <fvRsProv tnVzBrCPName="Contract2” > </fvRsProv>
        <cloudEPSelector name="sel1" matchExpression="custom:epgtag=='cloudepg1'" />
      </cloudEPg>

     </cloudApp>

      <vzFilter name="http" annotation="orchestrator:msc" >
      <vzEntry name="Entry3" prot="tcp" etherT="ipv4" arpOpc="unspecified" stateful="no"
applyToFrag="no" sFromPort="unspecified" sToPort="unspecified" dFromPort="80" dToPort="80" > </vzEntry>

    </vzFilter>
```

```
   <vzBrCP name="Contract2" scope="global">
      <vzSubj name="test-subj" >
        <vzRsSubjFiltAtt action="permit" tnVzFilterName="http" directives="none" />
        </vzSubj>
    </vzBrCP>
   </fvTenant>
</polUni>
```

# REST API を使用したクラウド EPG の作成

この例では、REST API を使用してクラウド EPG を作成する方法を示します。

### 始める前に

アプリケーション プロファイルと VRF を作成します。

クラウド EPG を作成するには、次の手順を実行します。

**例**：

```
<polUni>
  <fvTenant name="t2" status="">
    <!-- Tenant provide AWS credentials -->
   <cloudAwsProvider region="us-east-2" accessKeyId="123" secretAccessKey="ABCDE" providerId="admin"/>

    <fvCtx name="v1" status=""/>
    <cloudApp name="ap">
      <cloudEPg name="provEPG" status="">
        <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
        <cloudEPSelector name="1" matchExpression="custom:tag=='provfoo'"/>
        <cloudEPSelector name="2" matchExpression="custom:tag=='provbaz'"/>
        <fvRsProv tnVzBrCPName="httpFamily"/>
      </cloudEPg>
      <cloudEPg name="consEPG">
        <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
        <cloudEPSelector name="1" matchExpression="custom:tag=='consfoo'"/>
        <cloudEPSelector name="2" matchExpression="custom:tag=='consbaz'"/>
        <fvRsCons tnVzBrCPName="httpFamily"/>
      </cloudEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

# REST API を使用した外部クラウド EPG の作成

この例では、REST API を使用して外部クラウド EPG を作成する方法を示します。

### 始める前に

アプリケーション プロファイルと VRF を作成します。

外部クラウド EPG を作成するには、次の手順を実行します。

**例**：

```
<polUni>
  <fvTenant name="t2" status="">
    <!-- Tenant provide AWS credentials -->
   <cloudAwsProvider region="us-east-2" accessKeyId="123" secretAccessKey="ABCDE" providerId="admin"/>

    <fvCtx name="v1" status=""/>
    <cloudApp name="ap">
      <cloudEPg name="provEPGInternet" status="">
        <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
        <cloudEPSelector name="1" matchExpression="custom:tag=='provfoo'"/>
        <cloudEPSelector name="2" matchExpression="custom:tag=='provbaz'"/>
        <fvRsProv tnVzBrCPName="httpFamily"/>
      </cloudEPg>
      <cloudExtEPg name="consInternetEPG">
        <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
        <cloudExtEPSelector name="1" subnet="0.0.0.0/0"/>
        <fvRsCons tnVzBrCPName="httpFamily"/>
      </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

# REST API を使用したクラウド テンプレートの作成

このセクションでは、REST API を使用してクラウド テンプレートを作成する方法を示します。クラウド テンプレートの詳細については、クラウド テンプレートの概要 を参照してください。

REST API は、選択したライセンス モデルのタイプによって異なります。Cisco Catalyst 8000V のライセンス タイプは、`cloudtemplateProfile` 管理対象オブジェクトの `routerThroughput` プロパティによって取得されます。

`routerThroughput` 値が **T0/T1/T2/T3** に属している場合、**BYOL** Cisco Catalyst 8000V が Cisco Cloud APIC に展開されます。`routerThroughput` 値が **PAYG** の場合、**PAYG** Cisco Catalyst 8000V が Cisco Cloud APIC に展開されます。

**ステップ 1** **BYOL** Cisco Catalyst 8000V を展開するためのクラウド テンプレート ポストを作成するには、次の手順を実行します。

```
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
        <cloudtemplateProfile name="default" routerUsername="admin" routerPassword="rtpssw"
routerThroughput="15"
              routerLicenseToken="hYjZhYjItYTg0mrtrL15ocStS%0AUzRSZz0%3"
routerMgmtInterfacePublicIp="yes" routerDataInterfacePublicIp="yes"/>

      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>
```

```
      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="aws" region="us-west-1"/>
        <cloudRegionName provider="aws" region="us-west-2"/>
      </cloudtemplateIntNetwork>

      <cloudtemplateExtNetwork name="default">
        <cloudRegionName provider="aws" region="us-west-2"/>

        <cloudtemplateVpnNetwork name="default">

          <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />

          <cloudtemplateOspf area="0.0.0.1"/>

        </cloudtemplateVpnNetwork>

        <cloudtemplateBgpEvpn peeraddr="34.1.1.1/32" asn="63000" siteId="123" password="abcd1234"
/>

      </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```

（注） リリース 25.0(3) 以降、tier2（T2）は、Cisco Cloud APIC がサポートするデフォルトのスループットであり、上記の `cloudtemplateProfile` 管理対象オブジェクトの `routerThroughput` プロパティで示されます。

**ステップ 2** **PAYG** Cisco Catalyst 8000V を展開するためのクラウドテンプレート ポストを作成するには、次の手順を実行します。

```
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
         <cloudtemplateProfile name="default" routerUsername="admin" routerPassword="rtpssw"
routerThroughput="PAYG"
               vmName="c5.4xlarge" routerMgmtInterfacePublicIp="yes"
routerDataInterfacePublicIp="yes"/>

      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>

      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="aws" region="us-west-1"/>
        <cloudRegionName provider="aws" region="us-west-2"/>
      </cloudtemplateIntNetwork>

      <cloudtemplateExtNetwork name="default">
        <cloudRegionName provider="aws" region="us-west-2"/>

        <cloudtemplateVpnNetwork name="default">

          <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />

          <cloudtemplateOspf area="0.0.0.1"/>

        </cloudtemplateVpnNetwork>
```

```
        <cloudtemplateBgpEvpn peeraddr="34.1.1.1/32" asn="63000" siteId="123" password="abcd1234"
/>

      </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```

PAYG スループットを選択する場合、ユーザは、Cloud APIC によって作成され、管理対象オブジェクト `vmName` によって表される vmNames のリストから **vmName** も選択する必要があります。

次の表に、`cloudtemplateProfile` のプロパティ `vmName` によって示される vmNames を示します。

| AWS EC2 インスタンス | CCR スループット | vCPU の数 | メモリ |
|---|---|---|---|
| c5.xlarge | 最大 5 ギガビット スループット | 4 | 8 GiB |
| c5.2xlarge | 最大 10 ギガビット スループット | 8 | 16 GiB |
| c5.4xlarge | 最大 10 ギガビット スループット | 16 | 32 GiB |
| c5.9xlarge | 最大 10 ギガビット スループット | 36 | 72 GiB |
| c5n.xlarge | 最大 25 ギガビット スループット | 4 | 10.5 GiB |
| c5n.2xlarge | 最大 25 ギガビット スループット | 8 | 21 GiB |
| c5n.4xlarge | 最大 25 ギガビット スループット | 16 | 42 GiB |
| c5n.9xlarge | 最大 50 ギガビット スループット | 36 | 96 GiB |

# REST API を使用して VRF リーク ルートの構成

### 始める前に

このセクションの手順を実行する前に、内部 VRF 間のルート リーク と グローバルな Inter-VRF ルート リーク ポリシー に記載されている情報を確認してください。

**ステップ 1** 次のような投稿を入力して、契約ベースのルーティングを有効または無効にします。

```
<fvTenant name=”infra”>
    <cloudVrfRouteLeakPol name="default" allowContractBasedRouting=”true”/>
</fvTenant>
```

allowContractBasedRouting フィールドには、次のいずれかの設定があります。

- **true** : ルート マップがない場合、契約に基づいてルートが漏洩していることを示します。有効にすると、ルートマップが構成されていないときにコントラクトがルーティングを駆動します。ルートマップが存在する場合、ルート マップは常にルーティングを駆動します。
- **false**: デフォルト設定です。ルートが契約に基づいてリークされておらず、代わりにルート マップに基づいてリークされていることを示します。

**ステップ 2** 次のような投稿を入力して、leakInternalPrefix フィールドを使用して、VRF に関連付けられたすべてのクラウド CIDR のルート リークを設定します。

```
<fvTenant name=”t1”>
  <fvCtx name="v1">
    <leakRoutes>
      <leakInternalPrefix ip="0.0.0.0/0" le="32">
        <leakTo tenantName="t2" ctxName="v2" scope="public"/>
      </leakInternalPrefix>
    </leakRoutes>
  </fvCtx>
</fvTenant>

<fvTenant name=”t2”>
  <fvCtx name="v2">
    <leakRoutes>
      <leakInternalPrefix ip="0.0.0.0/0" le="32">
        <leakTo tenantName="t1" ctxName="v1" scope="public"/>
      </leakInternalPrefix>
    </leakRoutes>
  </fvCtx>
</fvTenant>
```

**ステップ 3** 次のような投稿を入力して、leakInternalSubnet フィールドを使用して、VRF のペア間の特定のルートをリークします。

```
<fvTenant name=”anyTenant" status="">
    <fvCtx name="VRF1" >
        <leakRoutes status="">
            <leakInternalSubnet ip="110.110.1.0/24" >
                <leakTo ctxName=”VRF2" scope="public" tenantName=" anyTenant " />
            </leakInternalSubnet>
        </leakRoutes>
    </fvCtx>
    <fvCtx name="VRF2" status="" >
        <leakRoutes status="">
            <leakInternalSubnet ip="110.110.2.0/24" >
                <leakTo ctxName=”VRF1" scope="public" tenantName=" anyTenant " />
            </leakInternalSubnet>
        </leakRoutes>
    </fvCtx>
</fvTenant>
```

# REST API を使用したトンネルのソース インターフェイス選択の構成

### 始める前に

このセクションの手順を実行する前に、トンネルのソース インターフェイスの選択 に記載されている情報を確認してください。

次のような投稿を入力して、トンネルの送信元インターフェイスの選択を構成します。

```
<cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
  <cloudtemplateProfile name="defaultxyz" routerUsername="james" routerPassword="bond@@7" />

  <cloudtemplateIpSecTunnelSubnetPool subnetpool="10.20.0.0/16" poolname="pool1" />

  <cloudtemplateIntNetwork name="default">
    <cloudRegionName provider="aws" region="us-west-1"/>
    <cloudRegionName provider="aws" region="us-west-2"/>
  </cloudtemplateIntNetwork>

  <cloudtemplateExtNetwork name="something” vrfName=”xyz” >
    <cloudRegionName provider="aws" region="us-west-2"/>
    <cloudtemplateVpnNetwork name="default">
      <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" poolname="" presharedkey=”abcd”
ikeVersion=”v1|v2”>
          <cloudtemplateIpSecTunnelSourceInterface sourceInterfaceId="2" />
      </cloudtemplateIpSecTunnel>
    </cloudtemplateVpnNetwork>
  </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。